SANbox 5802V
Fibre Channel Switch

Installation Guide

Firmware Version 7.2

59265-00 A

Information furnished in this manual is believed to be accurate and reliable. However, QLogic Corporation assumes no responsibility for its use, nor for any infringements of patents or other rights of third parties which may result from its use. QLogic Corporation reserves the right to change product specifications at any time without notice. Applications described in this document for any of these products are for illustrative purposes only. QLogic Corporation makes no representation nor warranty that such applications are suitable for the specified use without further testing or modification. QLogic Corporation assumes no responsibility for any errors that may appear in this document.

This SANbox switch is covered by one or more of the following patents: 6697359; other patents pending.

QLogic, SANbox, SANsurfer, Enterprise Fabric Suite 2007, QuickTools, and Multistage are trademarks or registered trademarks of QLogic Corporation.

Gnome is a trademark of the GNOME Foundation Corporation.

Java and Solaris are registered trademarks of Sun Microsystems, Inc.

Linux is a registered trademark of Linus Torvalds.

Mac OS X and Safari are registered trademarks of Apple Computer, Inc.

Microsoft, Windows XP, and Windows 2000/2003, and Internet Explorer are registered trademarks of Microsoft Corporation.

Netscape Navigator and Mozilla are trademarks or registered trademarks of Netscape Communications Corporation.

PowerPC is registered trademark of International Business Machines Corporation.

Red Hat is a registered trademark of Red Hat Software Inc.

S.u.S.E is a trademark of SUSE LINUX AG.

All other brand and product names are trademarks or registered trademarks of their respective owners.

Document Revision History

Release, Revision A, February 2008	Firmware Version 7.2

© 2008 QLogic Corporation. All Rights Reserved Worldwide.
First Published: November 2007

QLogic Corporation, 26650 Aliso Viejo Parkway, Aliso Viejo, CA 92656, (800) 662-4471 or (949) 389-6000

Table of Contents

1 Introduction

Intended Audience 1-1
Related Materials 1-2
Safety Notices 1-3
Sicherheitshinweise 1-3
Notes informatives relatives à la sécurité 1-3
Advertencias de seguridad 1-3
Communications Statements 1-4
- Federal Communications Commission (FCC) Class A Statement . . . 1-4
- Canadian Department of Communications Class A Compliance Statement 1-4
- Avis de conformité aux normes du ministère des Communications du Canada 1-4
- CE Statement 1-5
- VCCI Class A Statement 1-6

Laser Safety Information 1-6
Electrostatic Discharge Sensitivity (ESDS) Precautions 1-6
Accessible Parts 1-7
Pièces Accessibles 1-7
Zugängliche Teile 1-7
General Public License 1-8
- Preamble 1-8
- Terms And Conditions For Copying, Distribution And Modification . . . 1-9
- How to Apply These Terms to Your New Programs 1-13

Technical Support 1-15
- Availability 1-15
- Training 1-15
- Contact Information 1-16

2 General Description

Chassis Controls and LEDs 2-2
- Input Power LED (Green) 2-2
- Heartbeat LED (Green) 2-2
- System Fault LED (Amber) 2-2

Maintenance Button. 2-3
Resetting a Switch 2-3
Placing the Switch in Maintenance Mode 2-3
Fibre Channel Ports 2-4
Port LEDs 2-5
Port Logged-In LED (Green) 2-5
Port Activity LED (Green) 2-5
Transceivers 2-6
Port Types 2-6
Ethernet Port 2-7
Serial Port. 2-8
Power Supplies and Fans 2-9
Switch Management. 2-10
QuickTools Web Applet 2-10
Command Line Interface 2-10
Application Programming Interface 2-11
Simple Network Management Protocol 2-11
Storage Management Initiative–Specification (SMI-S) 2-11
File Transfer Protocols 2-11

3 Planning

Devices. 3-1
Device Access 3-2
Performance. 3-3
Distance. 3-3
Bandwidth 3-3
Latency 3-4
. . . . . .
Feature Licensing 3-5
Multiple Chassis Fabrics 3-6
Optimizing Device Performance 3-6
Domain ID, Principal Priority, and Domain ID Lock 3-7
Stacking 3-8
Common Topologies 3-11
Cascade Topology 3-11
Mesh Topology 3-12
MultiStage Topology 3-13
Switch Services 3-14
Fabric Security 3-15
Connection Security 3-16

User Account Security 3-17
Port Binding 3-17
Device Security 3-18
Security Example: Switches and HBAs with Authentication 3-19
Security Example: RADIUS Server 3-22
Security Example: Host Authentication 3-26
Fabric Management 3-28

4 Installation

Site Requirements 4-1
Fabric Management Workstation 4-2
Switch Power Requirements 4-2
Environmental Conditions 4-2
Installing a Switch 4-3
Mount the Switch 4-4
Install Transceivers 4-5
Configure the Workstation 4-7
Configuring the Workstation IP Address for Ethernet Connections 4-7
Configuring the Workstation Serial Port 4-8
Connect the Switch to AC Power 4-9
Connect the Workstation to the Switch 4-12
Configure the Switch 4-13
QuickTools Switch Configuration 4-13
CLI Switch Configuration 4-13
Cable Devices to the Switch 4-14
Installing Firmware 4-15
Using QuickTools to Install Firmware 4-16
Using the CLI to Install Firmware 4-16
One-Step Firmware Installation 4-16
Custom Firmware Installation 4-18
Adding a Switch to an Existing Fabric 4-19
Installing Feature License Keys 4-19

5 Diagnostics/Troubleshooting

Chassis Diagnostics 5-1
Input Power LED Is Extinguished 5-2
System Fault LED Is Illuminated 5-2
Power-On Self Test Diagnostics 5-3

Heartbeat LED Blink Patterns 5-3
Internal Firmware Failure Blink Pattern 5-4
Fatal POST Error Blink Pattern. 5-4
Configuration File System Error Blink Pattern 5-5
Over Temperature Blink Pattern 5-6
Logged-In LED Indications 5-7
E_Port Isolation 5-8
Excessive Port Errors 5-9
Transceiver Diagnostics 5-11
Power Supply Diagnostics 5-12
Recovering a Switch Using Maintenance Mode. 5-13
Exiting the Maintenance Menu (Option 0) 5-14
Unpacking a Firmware Image File in Maintenance Mode (Option 1) 5-14
Resetting the Network Configuration in Maintenance Mode (Option 2) 5-15
Resetting User Accounts in Maintenance Mode (Option 3). 5-15
Copying Log Files in Maintenance Mode (Option 4) 5-15
Removing the Switch Configuration in Maintenance Mode (Option 5) 5-15
Remaking the File System in Maintenance Mode (Option 6) 5-16
Resetting the Switch in Maintenance Mode (Option 7) 5-16
Updating the Boot Loader in Maintenance Mode (Option 8) 5-16

6 Removal/Replacement

Transceiver Removal and Replacement 6-2
Power Supply Removal and Replacement. 6-2

A Specifications

Fabric Specifications A-2
Maintainability. A-4
Fabric Management A-4
Dimensions. A-5
Electrical. A-5
Power Cord Specifications A-5
Environmental A-7
Regulatory Certifications A-8

Glossary

Index

List of Figures

Table		Page
2-1	SANbox 5802V Fibre Channel Switch	2-1
2-2	Chassis LEDs and Controls	2-2
2-3	Fibre Channel Ports	2-4
2-4	Port LEDs	2-5
2-5	Ethernet Port	2-7
2-6	Serial Port and Pin Identification	2-8
2-7	Power Supplies	2-9
3-1	Two-Switch Stack	3-8
3-2	Three-Switch Stack	3-8
3-3	Four-Switch Stack	3-9
3-4	Five Switch Stack	3-9
3-5	Six Switch Stack	3-10
3-6	Cascade-with-a-Loop Topology	3-11
3-7	Mesh Topology	3-12
3-8	Multistage Topology	3-13
3-9	Security Example: Switches and HBAs	3-19
3-10	Security Example: RADIUS Server	3-22
3-11	Security Example: Management Server	3-26
4-1	SANbox 5802V Fibre Channel	4-3
4-2	Removing XPAK Port Covers	4-6
4-3	Installing XPAK Switch Stacking Cables	4-6
4-4	Workstation Cable Connections	4-12
5-1	Chassis LEDs	5-1
5-2	Logged-In LED	5-7
5-3	Power Supply LEDs	5-12
6-1	Power Supply Removal	6-3
6-2	Power Supply Installation	6-3

List of Tables

Table		Page
2-1	Serial Port Pin Identification	2-8
3-1	Zoning Database Limits	3-2
3-2	Port-to-Port Latency	3-4
4-1	Management Workstation Requirements	4-2
A-1	Fabric Specifications	A-2
A-2	Maintainability Specifications	A-4
A-3	Fabric Management Specifications	A-4
A-4	Dimensional Specifications	A-5
A-5	Electrical Specifications	A-5
A-6	Availalbe Power Cords	A-5
A-7	Environmental Specifications	A-7
A-8	Regulatory Certifications	A-8

1 Introduction

This manual describes the features and installation of the SANbox® 5802V Fibre Channel switch, firmware version 7.2. This guide is organized as follows:

- Section 1 describes the intended audience, related materials, safety notices, communications statements, laser safety information, electrostatic discharge sensitivity precautions, accessible parts, general program license, and technical support.
- Section 2 is an overview of the switch. It describes indicator LEDs and all user controls and connections.
- Section 3 describes the factors to consider when planning a fabric.
- Section 4 explains how to install and configure the switch.
- Section 5 describes the diagnostic methods and troubleshooting procedures.
- Section 6 describes the removal and replacement of field replaceable units: media transceivers and power supplies.
- Appendix A lists the switch specifications.

Please read the communications statements and laser safety information later in this section.

Intended Audience

This manual introduces users to the switch and explains its installation and service. It is intended for users who are responsible for installing and servicing network equipment.

Related Materials

The following manuals and materials are referenced in the text and/or provide additional information.

- *SANbox 5802V Fibre Channel Switch Command Line Interface Guide*, publication number 59263-00.
- *SANbox Fibre Channel Switch CLI Quick Reference Guide Guide*, publication number 59261-01
- *SANbox 5802V QuickTools Switch Management User Guide*, publication number 59264-00.
- *QLogic Fibre Channel Switch Event Message Guide*, publication number 59060-04
- *SANbox Simple Network Management Protocol Reference Guide*, publication number, 59047-08
- *CIM Agent Reference Guide*, publication number 59223-02
- *QLogic Switch Interoperability Guide v3.0*. This PDF document can be downloaded at http://www.qlogic.com/interopguide/info.asp#inter.
- Fibre Channel-Arbitrated Loop (FC-AL-2) Rev. 6.8.
- Fibre Channel-10-bit Interface Rev. 2.3.
- Definitions of Managed Objects for the Fabric Element in Fibre Channel Standard (draft-ietf-ipfc-fabric-element-mib-04.txt).

The Fibre Channel Standards are available from:

Global Engineering Documents, 15 Inverness Way East, Englewood, CO 80112-5776 Phone: (800) 854-7179 or (303) 397-7956
Fax: (303) 397-2740.

Safety Notices

A **Warning** notice indicates the presence of a hazard that has the potential of causing personal injury.

4-4, 4-9, 6-1

A **Caution** notice indicates the presence of a hazard that has the potential of causing damage to the equipment.

4-5, 4-5, 5-16, 6-2

Sicherheitshinweise

Ein **Warnhinweis** weist auf das Vorhandensein einer Gefahr hin, die möglicherweise Verletzungen zur Folge hat.

4-4, 4-10, 6-1

Ein **Vorsichtshinweis** weist auf das Vorhandensein einer Gefahr hin, die möglicherweise Geräteschäden zur Folge hat.

4-5, 4-5, 5-16, 6-2

Notes informatives relatives à la sécurité

Une note informative **Avertissement** indique la présence d’un risque pouvant entraîner des blessures.

4-4, 4-9, 6-1

Une note informative **Attention** indique la présence d’un risque pouvant entraîner des dégâts matériels.

4-5, 4-5, 5-16, 6-2

Advertencias de seguridad

Un aviso de **Advertencia** indica la presencia de un peligro que puede causar lesiones personales.

4-4, 4-9, 6-1

Un aviso de **Precaución** indica la presencia de un peligro que puede causar daño al equipo.

4-5, 4-5, 5-16, 6-2

Communications Statements

The following statements apply to this product. The statements for other products intended for use with this product appear in their accompanying manuals.

Federal Communications Commission (FCC) Class A Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area may cause unacceptable interference, in which case the user will be required to correct the interference at their own expense.

Neither the provider nor the manufacturer is responsible for any radio or television interference caused by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

Canadian Department of Communications Class A Compliance Statement

This equipment does not exceed Class A limits for radio emissions for digital apparatus, set out in Radio Interference Regulation of the Canadian Department of Communications. Operation in a residential area may cause unacceptable interference to radio and TV reception requiring the owner or operator to take whatever steps necessary to correct the interference.

Avis de conformité aux normes du ministère des Communications du Canada

Cet équipement ne dépasse pas les limites de Classe A d'émission de bruits radioélectriques por les appareils numériques, telles que prescrites par le Réglement sur le brouillage radioélectrique établi par le ministère des Communications du Canada. L'exploitation faite en milieu résidentiel peut entraîner le brouillage des réceptions radio et télé, ce qui obligerait le propriétaire ou l'opérateur à prendre les dispositions nécwssaires pour en éliminer les causes.

CE Statement

The CE symbol on the equipment indicates that this system complies with the EMC (Electromagnetic Compatibility) directive of the European Community (2004/108/EC) and to the Low Voltage (Safety) Directive (2006/95/EC). Such marking indicates that this system meets or exceeds the following technical standards:

- EN 60950-1:2001 – “Safety of Information Technology Equipment”.
- EN 55022:2006 Class A – “Limits and Methods of Measurement of Radio Interference Characteristics of Information Technology Equipment”.
- EN 55024:1998, A1:2001, A2: 2003 – “Electromagnetic compatibility - Generic immunity standard Part 1: Residential commercial, and light industry.”
  - EN 61000-4-2: 1995, A1:1998, A2: 2001 – “Electrostatic Discharge Immunity Test”
  - EN 61000-4-3:2002 – “Radiated, Radio-Frequency, Electromagnetic Field Immunity Test”
  - EN 61000-4-4:2004 – “Electrical Fast Transient/Burst Immunity Test”
  - EN 61000-4-5:1995, A1:2001 – “Surge Immunity Test”
  - EN 61000-4-6:1996, A1:2001 – “Immunity To Conducted Disturbances, Induced By Radio-Frequency Fields”
  - EN 61000-4-8:1993, A1:2001 – "Power Frequency Magnetic Field Immunity Test”
  - EN 61000-4-11 Second Edition: 2004 – “Voltage Dips, Short Interruptions And Voltage Variations Immunity Tests”
- EN 61000-3-2:2000 A2 :2005 – “Limits For Harmonic Current Emissions (Equipment Input Current Less Than/Equal To 16 A Per Phase)” Class A
- EN 61000-3-3: 1995, A1:2001 – “Limitation Of Voltage Fluctuations And Flicker In Low-Voltage Supply Systems For Equipment With Rated Current Less Than Or Equal To 16 A”

VCCI Class A Statement

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

This is a Class A product based on the standard of the Voluntary Control Council For Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

Laser Safety Information

This product uses Class 1 laser optical transceivers to communicate over the fiber optic conductors. The U.S. Department of Health and Human Services (DHHS) does not consider Class 1 lasers to be hazardous. The International Electrotechnical Commission (IEC) 825 Laser Safety Standard requires labeling in English, German, Finnish, and French stating that the product uses Class 1 lasers. Because it is impractical to label the transceivers, the following label is provided in this manual.

Electrostatic Discharge Sensitivity (ESDS) Precautions

The assemblies used in the switch chassis are ESD sensitive. Observe ESD handling procedures when handling any assembly used in the switch chassis.

Accessible Parts

The Field Replaceable Units (FRUs) for the SANbox 5802V switch are the following:

- Power supplies
- Small Form-Factor Pluggable (SFP) optical transceivers
- XPAK optical transceivers

Pièces Accessibles

Les pièces remplaçables, Field Replaceable Units (FRU), du commutateur SANbox 5802V Fibre Channel Switch sont les suivantes:

- Alimentations de courant
- Interfaces aux media d’interconnexion appelés SFP transceivers.
- Interfaces aux media d’interconnexion appelés XPAK transceivers.

Zugängliche Teile

Nur die folgenden Teile im SANbox 5802V Fibre Channel Switch können kundenseitig ersetzt werden:

- Netzteile
- Schnittstellen für die Zwischenverbindungsträger, SFP transceivers genannt.
- Schnittstellen für die Zwischenverbindungsträger, XPAK transceivers genannt.

General Public License

QLogic® Fibre Channel switches are powered by the Linux operating system. A machine-readable copy of the Linux source code is available upon written request to the following address. A nominal fee will be charged for reproduction, shipping, and handling costs in accordance with the General Public License.

QLogic Corporation
6321 Bury Drive
Eden Prairie, MN 55346-1739
Attention: Technical Support - Source Request

Warning: Installation of software or files not authorized by QLogic will immediately and irrevocably void all warranty and service contracts on the affected units.

The following general public license has been reproduced with permission from:

GNU General Public License
Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

Terms And Conditions For Copying, Distribution And Modification

1. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

2. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

3. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

   These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

   Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

   In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

4. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1

and 2 above on a medium customarily used for software interchange; or,

b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

5. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

6. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

7. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

8. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

   This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

9. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

10. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

11. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

12. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

13. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

14. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.

Copyright (C) *yyyy name of author*

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) *year name of author*

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

signature of Ty Coon, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

Technical Support

Customers should contact their authorized maintenance provider for technical support of their QLogic switch products. QLogic-direct customers may contact QLogic Technical Support; others will be redirected to their authorized maintenance provider.

Visit the QLogic support Web site listed in Contact Information for the latest firmware and software updates.

Availability

QLogic Technical Support for products under warranty is available during local standard working hours excluding QLogic Observed Holidays.

Training

QLogic offers certification training for the technical professional for both the SANblade™ HBAs and the SANbox switches. From the training link at www.qlogic.com, you may choose Electronic-Based Training or schedule an intensive "hands-on" Certification course.

Technical Certification courses include installation, maintenance and troubleshooting QLogic SAN products. Upon demonstrating knowledge using live equipment, QLogic awards a certificate identifying the student as a Certified Professional. The training professionals at QLogic may be reached by email at tech.training@qlogic.com.

Contact Information

Support Headquarters	QLogic Corporation 12984 Valley View Road Eden Prairie, MN 55344-3657 USA
QLogic Web Site	www.qlogic.com
Technical Support Web Ste	support.qlogic.com
Technical Support Email	support@qlogic.com
Technical Training Email	tech.training@qlogic.com
North American Region	
Email	support@qlogic.com
Phone	+1-952-932-4040
Fax	+1 952-974-4910
Europe, Middle East, and Africa Region	
Email	emeasupport@qlogic.com
Phone Numbers by Language	+353 1 6924960 - English +353 1 6924961 - Français +353 1 6924962 - Deutsch +353 1 6924963 - Español +353 1 6924964 - Português +353 1 6924965 - Italiano
Asia Pacific Region	
Email	apacsupport@qlogic.com
Phone Numbers by Language	+63-2-885-6712 - English +63-2-885-6713 - (Mandarin) +63-2-885-6714 - (Japanese) +63-2-885-6715 - (Korean)
Latin and South America Region	
Email	calasupport@qlogic.com
Phone Numbers by Language	+52 55 5278 7016 - English +52 55 5278 7017 - Español +52 55 5278 7015 - Português

2 General Description

The SANbox 5802V switch, shown in Figure 2-1, is a 24-port 8-Gbps Fibre Channel switch with both Ethernet and serial management interfaces. This section describes the features and capabilities of the SANbox 5802V switch and includes information about the following features:

- Chassis Controls and LEDs
- Fibre Channel Ports
- Ethernet Port
- Power Supplies and Fans
- Switch Management

Fabrics are managed with the Command Line Interface (CLI) or the QuickTools web applet.

- Refer to *SANbox 5802V Fibre Channel Switch Command Line Interface Guide* for more information about the CLI.
- Refer to the *SANbox 5802V QuickTools Switch Management User Guide* for information about QuickTools.

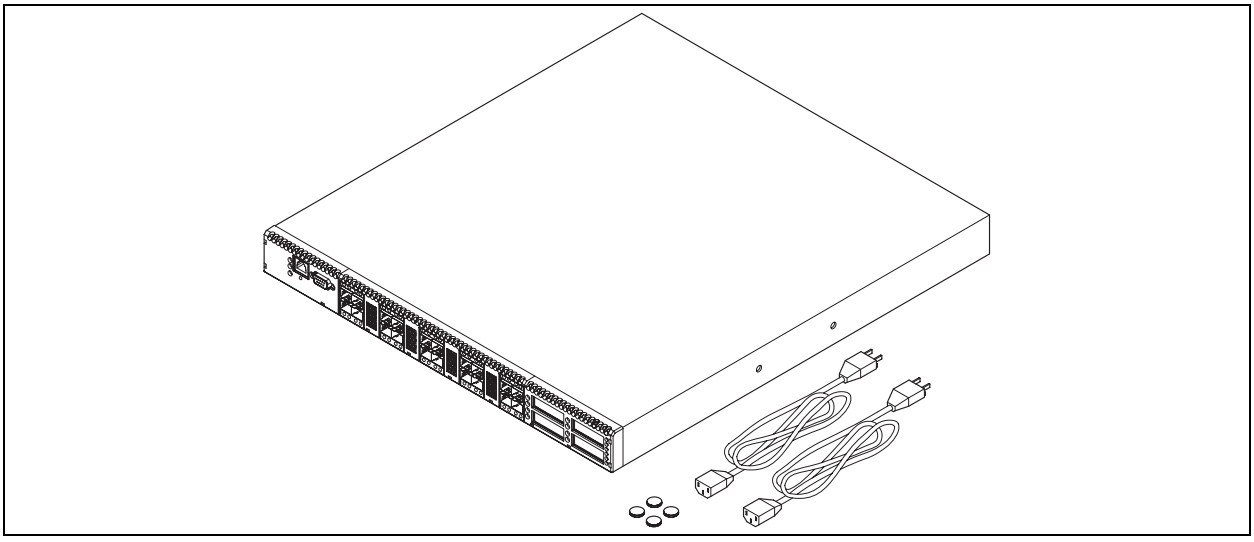


Figure 2-1 SANbox 5802V Fibre Channel Switch

Chassis Controls and LEDs

The chassis LEDs provide information about the switch's operational status. These LEDs include the Input Power LED (green), Heartbeat LED (green), and the System Fault LED (amber) as shown in Figure 2-2. The Maintenance button shown in Figure 2-2 is the only chassis control and is used to reset a switch or to recover a disabled switch. To apply power to the switch, plug the power cords into the switch AC power receptacles, located on the back of the switch, and into a 100–240 VAC power source.

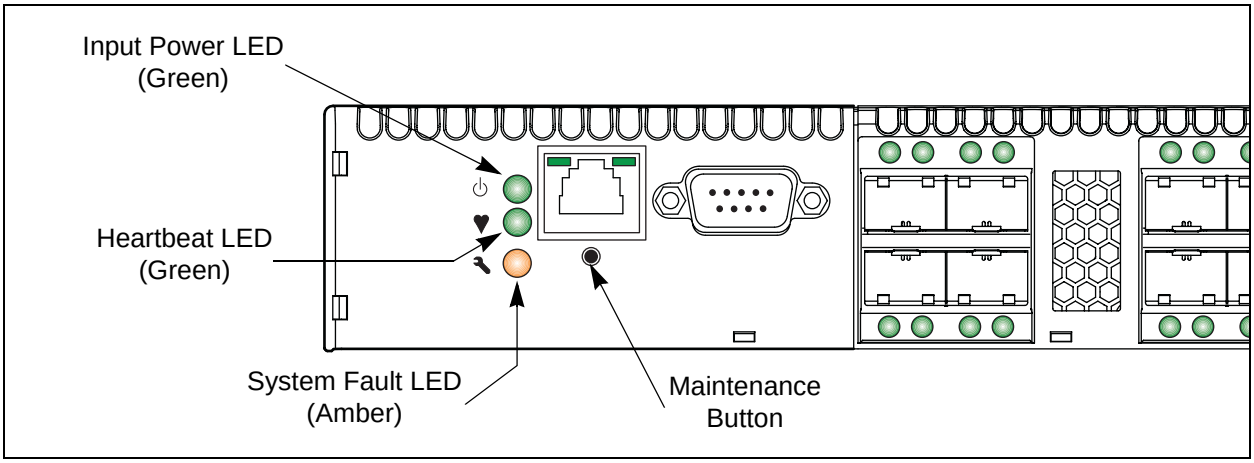


Figure 2-2 Chassis LEDs and Controls

Input Power LED (Green)

The Input Power LED indicates the voltage status at the switch logic circuitry. During normal operation, this LED illuminates to indicate that the switch logic circuitry is receiving the proper DC voltages. When the switch is in maintenance mode, this LED is extinguished.

Heartbeat LED (Green)

The Heartbeat LED indicates the status of the internal switch processor and the results of the POST. Following a normal power-up, the Heartbeat LED blinks about once per second to indicate that the switch passed the POST and that the internal switch processor is running. In maintenance mode, the Heartbeat LED illuminates continuously. Refer to "Heartbeat LED Blink Patterns" on page 5-3 for more information about Heartbeat LED blink patterns.

System Fault LED (Amber)

The System Fault LED illuminates to indicate that a fault exists in the switch firmware or hardware. Fault conditions include POST errors, over-temperature conditions, and power supply malfunctions. The Heartbeat LED shows a blink code for POST errors and over temperature conditions. For more information, refer to "Heartbeat LED Blink Patterns" on page 5-3.

Maintenance Button

The Maintenance button, shown in Figure 2-2, is a dual-function momentary switch on the front panel. Its purpose is to reset the switch or to place the switch in maintenance mode. Maintenance mode sets the IP address to 10.0.0.1 and provides access to the switch for maintenance purposes when flash memory or the resident configuration file is corrupted. Refer to “Recovering a Switch Using Maintenance Mode” on page 5-13 for more information.

Resetting a Switch

To reset the switch, press and hold the Maintenance button for less than 2 seconds. The switch will respond as follows:

1. All the chassis LEDs will illuminate except the System Fault LED.
2. After approximately 1 minute, the power-on self test (POST) begins, extinguishing the Heartbeat LED.
3. When the POST is complete, the Input Power LED is illuminated and the Heartbeat LED is flashing once per second.

Placing the Switch in Maintenance Mode

To place the switch in maintenance mode, do the following:

1. Isolate the switch from the fabric.
2. Press and hold the Maintenance button with a pointed tool for a few seconds until only the Heartbeat LED is illuminated. Continue holding the maintenance button until the Heartbeat LED extinguishes, then release the button. The Heartbeat LED illuminates continuously while the switch is in maintenance mode.

To exit maintenance mode and return to normal operation, press and release the Maintenance button momentarily to reset the switch.

Fibre Channel Ports

The SANbox 5802V switch has twenty Fibre Channel Small Form-Factor Pluggable (SFP) ports and four Fibre Channel XPAK ports. SFP ports are numbered 0–19 as shown in Figure 2-3. Each SFP port is served by an SFP optical transceiver and is capable of 2-, 4-, or 8-Gbps transmission. SFP ports are hot-pluggable and can self-discover both the port type and transmission speed when connected to devices or other switches. The port LEDs are located above ports 0–9 and below ports 10–19, and provide port login and activity status information.

The XPAK ports are numbered 20–23 as shown in Figure 2-3. Each XPAK port is served by an XPAK optical transceiver or an XPAK switch stacking cable and is capable of 10-Gbps transmission. XPAK ports are hot-pluggable and can self-discover transmission speed when connected to devices or other switches. The XPAK switch stacking cable is a passive cable and transceiver assembly for connecting to other XPAK-capable switches. The XPAK ports come from the factory with covers that must be removed before installing transceivers or cables. XPAK port LEDs are located to the left of their respective ports and provide port login and activity status.

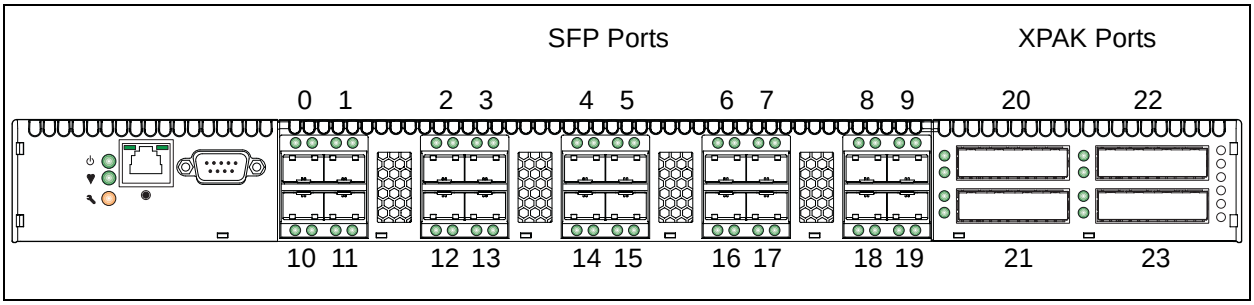


Figure 2-3 Fibre Channel Ports

The SANbox 5802V switch comes from the factory as a 12-port switch, enabling SFP ports 0–7 and XPAK ports 20–23. You can activate additional SFP ports and upgrade the XPAK ports to 20-Gbps with the purchase of license keys. For more information, refer to “Feature Licensing” on page 3-5.

Port LEDs

Each port has its own Logged-In LED (L) and Activity LED (A) as shown in Figure 2-4.

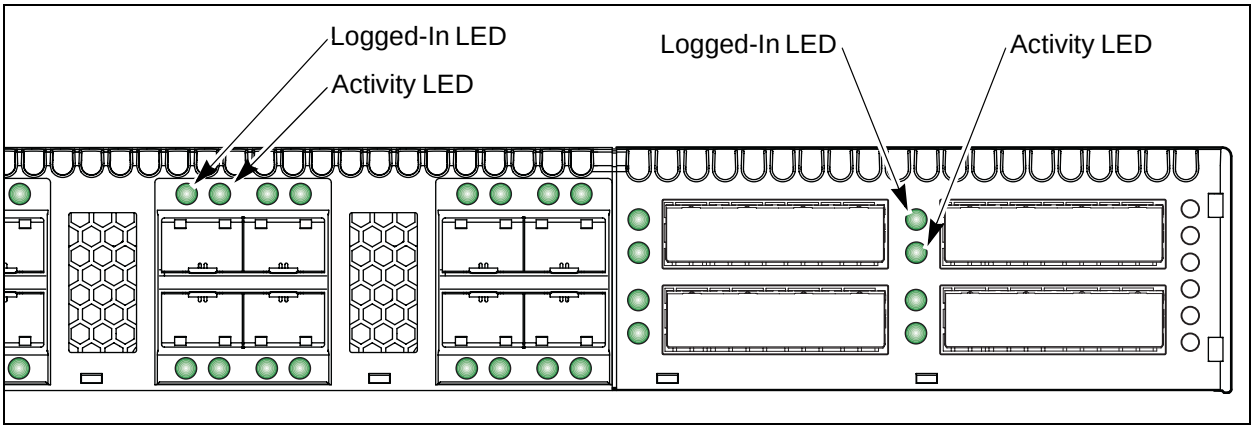


Figure 2-4 Port LEDs

Port Logged-In LED (Green)

The Logged-in LED indicates the logged-in or initialization status of the connected devices. After successful completion of the POST, the switch extinguishes all Logged-In LEDs. Following a successful port login, the switch illuminates the corresponding logged-in LED. This shows that the port is properly connected and able to communicate with its attached devices. The Logged-In LED remains illuminated as long as the port is initialized or logged in. If the port connection is broken or an error occurs that disables the port, the Logged-In LED is extinguished. Refer to “Logged-In LED Indications” on page 5-7 for more information about the Logged-In LED.

Port Activity LED (Green)

The Activity LED indicates that data is passing through the port. Each frame that the port transmits or receives illuminates this LED for 50 milliseconds. This makes it possible to observe the transmission of a single frame.

Transceivers

The SANbox 5802V switch supports SFP optical transceivers for the SFP ports and XPAK optical transceivers or XPAK stacking cables for the XPAK ports. A transceiver converts electrical signals to and from optical laser signals to transmit and receive data. Duplex fiber optic cables plug into the SFP transceivers which then connect to the devices. An SFP port is capable of transmitting at 2-, 4-, or 8-Gbps; however, the transceiver must also be capable of delivering at these rates.

The SFP and XPAK transceivers are hot-pluggable. This means that you can remove or install a transceiver while the switch is operating without harming the switch or the transceiver. However, communication with the connected device will be interrupted. Refer to “Install Transceivers” on page 4-5 for information about installing and removing SFP and XPAK optical transceivers.

Port Types

SANbox 5802V switches support generic ports (G_Port, GL_Port), fabric ports (F_Port, FL_Port), and expansion ports (E_Port). Switches come from the factory with all SFP ports configured as GL_Ports. The XPAK ports come from the factory configured as G_Ports. Generic, fabric, and expansion ports function as follows:

- A GL_Port self-configures as an FL_Port when connected to a loop device, as an F_Port when connected to a single device, or as an E_Port when connected to another switch. If the device is a single device on a loop, the GL_Port will attempt to configure first as an F_Port, then if that fails, as an FL_Port.
- A G_Port self-configures as an F_Port when connected to a single device, or as an E_Port when connected to another switch.
- An FL_Port supports a loop of up to 126 devices. An FL_Port can also configure itself during the fabric login process as an F_Port when connected to a single device (N_Port).
- An F_Port supports a single device.
- E_Ports enable you to expand the fabric by connecting SANbox 5802V switches.

SANbox 5802V switches self-discover all inter-switch connections. Refer to “Multiple Chassis Fabrics” on page 3-6 for more information.

Ethernet Port

The Ethernet port is an RJ-45 connector that provides a connection to a management workstation through a 10/100 Base-T Ethernet cable as shown in Figure 2-5. A management workstation can be a Windows®, Solaris™, or a Linux® workstation that is used to configure and manage the switch fabric. You can manage the switch over an Ethernet connection using the CLI, QuickTools, or SNMP.

The Ethernet port has two LEDs: the Link Status LED (green) and the Activity LED (green). The Link Status LED illuminates continuously when an Ethernet connection has been established. The Activity LED illuminates when data is being transmitted or received over the Ethernet connection.

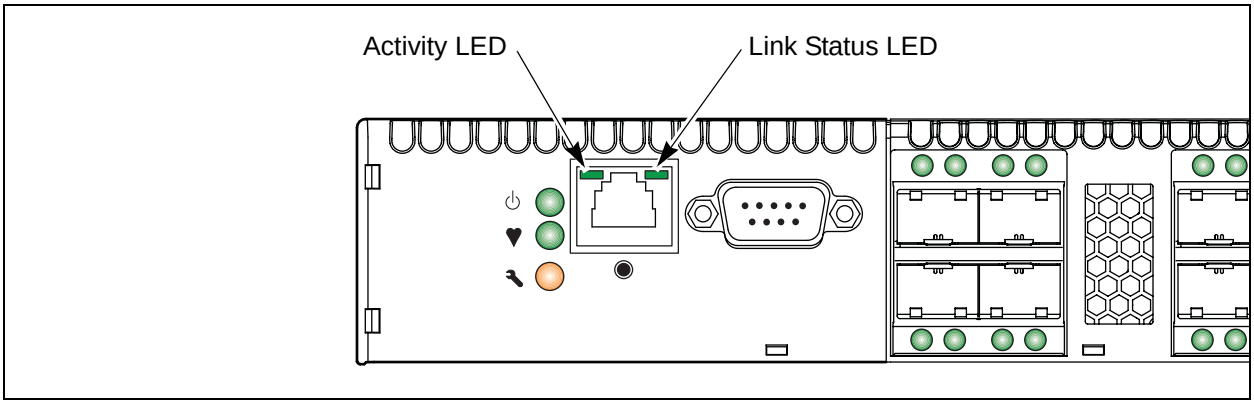


Figure 2-5 Ethernet Port

Serial Port

The SANbox 5802V switch is equipped with an RS-232 serial port for maintenance purposes as shown in Figure 2-6. You can manage the switch through the serial port using the CLI.

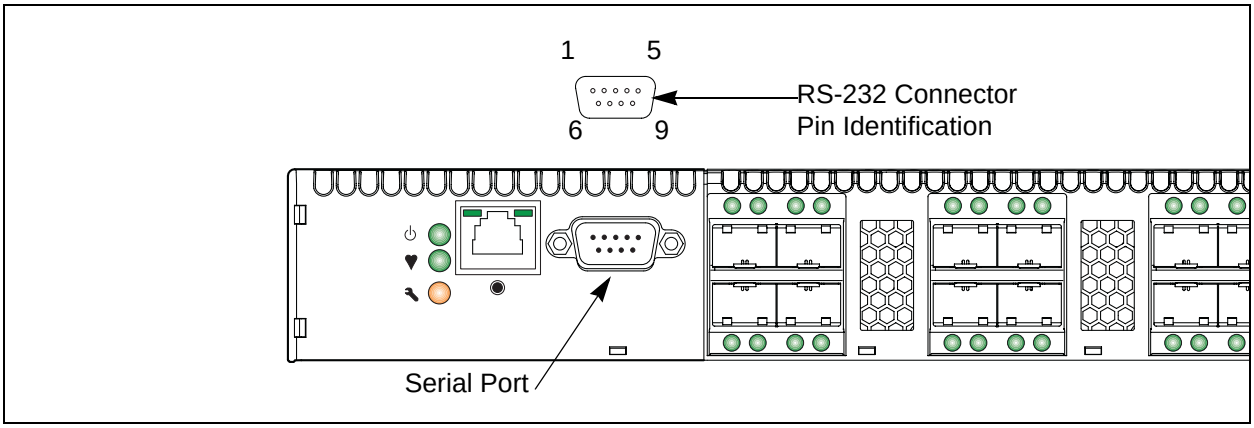


Figure 2-6 Serial Port and Pin Identification

The serial port requires a null-modem F/F DB9 cable. The pins on the switch RS-232 connector are shown in Figure 2-6 and identified in Table 2-1. Refer to "Connect the Workstation to the Switch" on page 4-12 for information about connecting the management workstation through the serial port.

Table 2-1. Serial Port Pin Identification

Pin Number	Description
1	Carrier Detect (DCD)
2	Receive Data (RxD)
3	Transmit Data (TxD)
4	Data Terminal Ready (DTR)
5	Signal Ground (GND)
6	Data Set Ready (DSR)
7	Request to Send (RTS)
8	Clear to Send (CTS)
9	Ring Indicator (RI)

Power Supplies and Fans

The model 5802V switch has two, hot pluggable power supplies that convert standard 100–240 VAC to DC voltages for the various switch circuits. Each power supply has an AC power receptacle and two status LEDs as shown in Figure 2-7:

- The Power Supply Status LED (green) illuminates to indicate that the power supply is receiving AC voltage and producing the proper DC voltages.
- The Power Supply Fault LED (amber) illuminates to indicate that a power supply fault exists and requires attention.

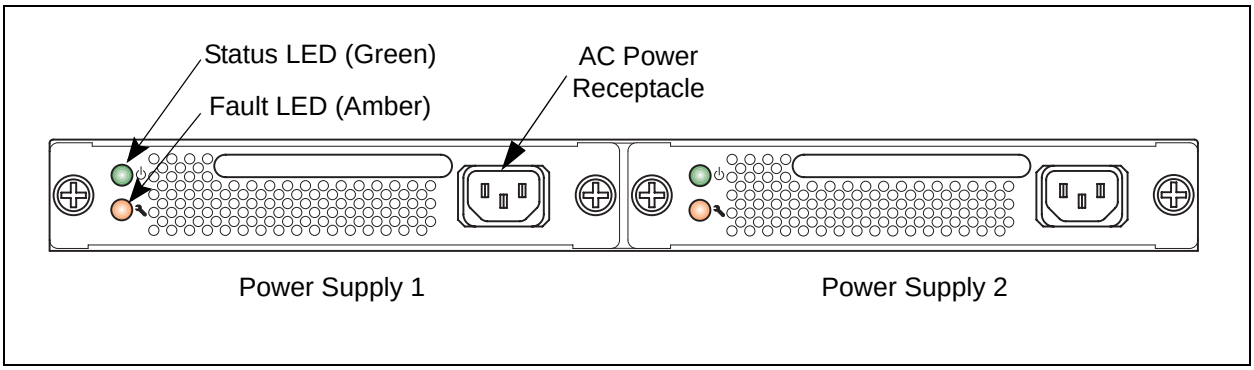


Figure 2-7 Power Supplies

Switch Management

The switch supports the following management tools:

- QuickTools Web Applet
- Command Line Interface
- Application Programming Interface
- Simple Network Management Protocol
- Storage Management Initiative–Specification (SMI-S)
- File Transfer Protocols

QuickTools Web Applet

QuickTools is a browser-based graphical user interface (GUI) that provides basic switch management tools. You run QuickTools by opening the switch IP address with an internet browser. QuickTools provides the following management features:

- Faceplate device management
- Switch and port statistics
- Configuration wizard
- Zoning administration
- Fabric tree for fabric management
- User account configuration
- Switch and fabric events
- Operational and environmental statistics
- Global device nicknames
- Online help

For more information, refer to the *SANbox 5802V QuickTools Switch Management User Guide*.

Command Line Interface

The command line interface (CLI) provides monitoring and configuration functions by which the administrator can manage the fabric and its switches. The CLI is available over an Ethernet connection or a serial connection. Refer to *SANbox 5802V Fibre Channel Switch Command Line Interface Guide* for more information.

Application Programming Interface

The Application Programming Interface (API) enables an application provider to build a management application for QLogic switches. The library is implemented in ANSI standard C, relying only on standard POSIX run-time libraries. Contact your distributor or authorized reseller for information about the API.

Simple Network Management Protocol

SNMP provides monitoring and trap functions for the fabric. SANbox firmware supports SNMP versions 1 and 2, the Fibre Alliance Management Information Base (FA-MIB) version 4.0, and the Fabric Element Management Information Base (FE-MIB) RFC 2837. Traps can be formatted using SNMP version 1 or 2. Refer to the *SANbox Simple Network Management Protocol Reference Guide* for more information.

Storage Management Initiative–Specification (SMI-S)

SMI-S provides for the management of the switch through third-party applications that use the SMI-S. Refer to the *CIM Agent Reference Guide* for more information.

File Transfer Protocols

FTP and TFTP provide the command line interface for exchanging files between the switch and the management workstation. These files include firmware image files, configuration files, and log files.

Notes

3 Planning

Consider the following when planning a fabric:

- Devices
- Device Access
- Performance
- Feature Licensing
- Multiple Chassis Fabrics
- Switch Services
- Fabric Security
- Fabric Management

Devices

When planning a fabric, consider the number of devices and the anticipated demand. This will determine the number of ports that are needed and in turn the number of switches.

Consider the transmission speeds of your HBAs and SFPs. The switch ports 0–19 support 2-Gbps, 4-Gbps, and 8-Gbps transmission speeds.

Consider also the distribution of targets and initiators. An F_Port supports a single device. An FL_Port can support up to 126 devices in an arbitrated loop.

Device Access

Consider device access needs within the fabric. Access is controlled by the use of zoning. Some zoning strategies include the following:

- Separate devices by operating system.
- Separate devices that have no need to communicate with other devices in the fabric or have classified data.
- Separate devices into department, administrative, or other functional group.
- Reserve a path and its bandwidth from one port to another.

Zoning divides the fabric for purposes of controlling discovery and inbound traffic. A zone is a named group of ports or devices. Members of the same zone can communicate with each other and transmit outside the zone, but cannot receive inbound traffic from outside the zone. Zoning is hardware-enforced only when a port/device is a member of no more than eight zones whose combined membership does not exceed 64. If this condition is not satisfied, that port behaves as a soft zone member. You can assign ports/devices to a zone individually or as a group by creating an alias.

A zone can be a component of more than one zone set. Several zone sets can be defined for a fabric, but only one zone set can be active at one time. The active zone set determines the current fabric zoning.

A zoning database is maintained on each switch. Table 3-1 describes the zoning database limits, excluding the active zone set.

Table 3-1. Zoning Database Limits

Limit	Description
MaxZoneSets	Maximum number of zone sets (256).
MaxZones	Maximum number of zones (2000).
MaxAliases	Maximum number of aliases (2500).
MaxTotalMembers	Maximum number of zone and alias members (10000) that can be stored in the zoning database. Each instance of a zone member or alias member counts toward this maximum.
MaxZonesInZoneSets	Maximum number of zones that are components of zone sets (2000), excluding the orphan zone set. Each instance of a zone in a zone set counts toward this maximum.
MaxMembersPerZone	Maximum number of members in a zone (2000).
MaxMembersPerAlias	Maximum number of members in an alias (2000)

Performance

The SANbox 5802V switch supports class 2 and class 3 Fibre Channel service at transmission rates of 2-, 4-, 8-,10-, or 20-Gbps with a maximum frame size of 2148 bytes. Each Fibre Channel port adapts its transmission speed to match that of the device to which it is connected prior to login when the connected device powers up. Related performance characteristics include the following:

- Distance
- Bandwidth
- Latency

Distance

Consider the physical distribution of devices and switches in the fabric. Choose SFP transceivers that are compatible with the cable type, distance, Fibre Channel revision level, and the device host bus adapter. Refer to Appendix A for more information about cable types and transceivers.

Each Fibre Channel SFP port is supported by a data buffer with a 16 credit capacity; that is, 16 maximum sized frames. For fiber optic cables, this enables full bandwidth over the following approximate distances:

- 13 kilometers at 2-Gbps (1.2 credits/Km)
- 6 kilometers at 4-Gbps (2.4 credits/km)
- 3 kilometers at 8-Gbps (4.8 credits/Km)

Bandwidth

Bandwidth is a measure of the volume of data that can be transmitted at a given transmission rate. An SFP port can transmit or receive at nominal rates of 2-, 4-, or 8-Gbps depending on the device to which it is connected. This corresponds to full duplex bandwidth values of 424 MB, 850 MB, and 1700 MB respectively. XPAK ports transmit at a nominal rate of 10-Gbps which corresponds to a full duplex bandwidth value of 2550 MB. With a 20-Gbps license key, XPAK ports can transmit at a nominal rate of 20-Gbps (5100 MB bandwidth).

Multiple source ports can transmit to the same destination port if the destination bandwidth is greater than or equal to the combined source bandwidth. For example, two 2-Gbps source ports can transmit to one 4-Gbps destination port. Similarly, one source port can feed multiple destination ports if the combined destination bandwidth is greater than or equal to the source bandwidth.

In multiple chassis fabrics, each link between chassis contributes 424, 850, 1700, 2550, or 5100 megabytes of bandwidth between those chassis, depending on the speed of the link. When additional bandwidth is needed between devices, increase the number of links between the connecting switches. The switch guarantees in-order delivery with any number of links between chassis.

Latency

Latency is a measure of how fast a frame travels through a switch from one port to another. The factors that affect latency include transmission rate and the source/destination port relationship as shown in Table 3-2.

Table 3-2. Port-to-Port Latency

	Destination Rate					
Source Rate	Gbps	2	4	8	10	20
	2	< 0.6 µsec	< 0.7 µsec[1]	< 0.6 µsec[1]	< 0.6 µsec[1]	< 0.6 µsec[1]
	4	< 0.4 µsec	< 0.3 µsec	< 0.4 µsec[1]	< 0.4 µsec[1]	< 0.3 µsec[1]
	8	< 0.3 µsec	< 0.2 µsec	< 0.2 µsec	< 0.2 µsec[1]	< 0.2 µsec[1]
	10	< 0.3 µsec	< 0.3 µsec	< 0.2 µsec	< 0.2 µsec	< 0.2 µsec[1]
	20	< 0.3 µsec	< 0.2 µsec	< 0.2 µsec	< 0.2 µsec	< 0.2 µsec

[1] Based on minimum frame size of 36 bytes. Latency increases for larger frame sizes.

Feature Licensing

NOTE:

License keys enable commands and keywords in the CLI. License keys do not affect the capabilities of the QuickTools web applet.

License keys provide a way to expand the capabilities of your switch and fabric as your needs grow. Consider your need for the following features and arrange to purchase license keys from your switch distributor or authorized reseller.

- Fabric Security provides access to the following security tools:
  - Security for Ethernet connections using the Secure Socket Layer (SSL) protocol and Telnet connections using the Secure Shell (SSH) protocol
  - Device and switch authorization and authentication using the Challenge Handshake Authentication Protocol (CHAP).
  - Remote authentication of users and devices using the Remote Authentication Dial-In User Service (RADIUS)
- SANdoctor provides access to the following tools:
  - Fibre Channel connection verification (Fcping CLI command)
  - Fibre Channel route tracing (Fctrace CLI command)
  - Transceiver diagnostic information (Show Media CLI command).
- Port Activation activates additional SFP ports for a total of 12, 16, or 20 ports.
- 20-Gbps license enables the XPAK ports to transmit and receive at 20-Gbps instead of the default 10-Gbps.

Upgrading a switch is not disruptive, nor does it require a switch reset. To order a license key, contact your switch distributor or your authorized reseller. Refer to “Installing Feature License Keys” on page 4-19 for information about installing a license key.

Multiple Chassis Fabrics

By connecting switches together you can expand the number of available ports for devices. Each switch in the fabric is identified by a unique domain ID, and the fabric can automatically resolve domain ID conflicts. Because the Fibre Channel ports are self-configuring, you can connect SANbox 5802V switches together in a wide variety of topologies.

You can connect up to six SANbox 5802V switches together through the XPAK ports, thus preserving the SFP ports for devices. This is called stacking. SANbox 5802V switches divide the XPAK port buffer to balance traffic across the connection. The XPAK ports operate with any standard XPAK interface. You can also connect SANbox 5802V switches with other switches through the SFP ports in a wide variety of topologies. Consider your topology and cabling requirements.

Optimizing Device Performance

When choosing a topology for a multiple chassis fabric, you should also consider the locality of your server and storage devices and the performance requirements of your application. Storage applications such as video distribution, medical record storage/retrieval or real-time data acquisition can have specific latency or bandwidth requirements.

The SANbox 5802V switch provides the lowest latency of any product in its class. Refer to “Performance” on page 3-3 for information about latency. However, the highest performance is achieved on Fibre Channel switches by keeping traffic within a single switch instead of relying on ISLs. Therefore, for optimal device performance, place devices on the same switch under the following conditions:

- Heavy I/O traffic between specific server and storage devices.
- Distinct speed mismatch between devices such as the following:
  - A 8-Gbps server and a slower 4-Gbps storage device
  - A high performance server and slow tape storage device

Domain ID, Principal Priority, and Domain ID Lock

The following switch configuration settings affect multiple chassis fabrics:

- Domain ID
- Principal priority
- Domain ID lock

The domain ID is a unique number from 1–239 that identifies each switch in a fabric. The principal priority is a number (1–255) that determines the principal switch which manages domain ID assignments for the fabric. The switch with the highest principal priority (1 is high, 255 is low) becomes the principal switch. If the principal priority is the same for all switches in a fabric, the switch with the lowest WWN becomes the principal switch.

The domain ID lock allows (False) or prevents (True) the reassignment of the domain ID on that switch. Switches come from the factory with the domain ID set to 1, the domain ID lock set to False, and the principal priority set to 254. Refer to the Set Config Switch command in the *SANbox 5802V Fibre Channel Switch Command Line Interface Guide* for information about changing the default domain ID, domain ID lock, and principal priority parameters.

If you connect a new switch to an existing fabric with its domain ID unlocked, and a domain ID conflict occurs, the new switch will isolate as a separate fabric. However, you can remedy this by resetting the new switch or taking it offline then putting it back online. The principal switch will reassign the domain ID and the switch will join the fabric.

NOTE:

Domain ID reassignment is not reflected in zoning that is defined by domain ID/port number pair or Fibre Channel address. You must reconfigure zones that are affected by domain ID reassignment. To prevent zoning definitions from becoming invalid under these conditions, lock the domain IDs. Domain ID reassignment has no effect on zone members defined by WWN.

Stacking

You can connect up to six SANbox 5802V switches together through the XPAK ports, thus preserving the SFP ports for devices. This is called stacking. The following 2-, 3-, 4-, 5-, and 6-switch stacking configurations are recommended for best performance and redundancy. Each XPAK port at 10-Gbps contributes 1 GB of bandwidth between chassis with one chassis hop between any two ports. Figure 3-1 shows a two-switch stack of model 5802V switches using two 3-inch XPAK switch stacking cables. Forty SFP ports are available for devices.

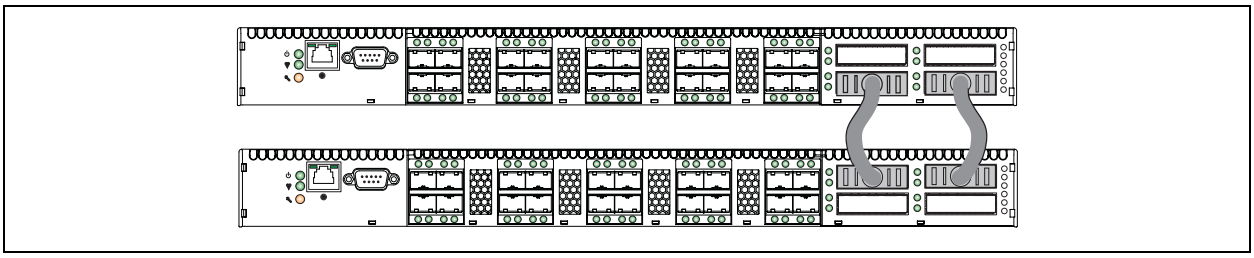


Figure 3-1 Two-Switch Stack

Figure 3-2 shows a three-switch stack of SANbox 5802V switches using two 3-inch and one 9-inch XPAK switch stacking cables. Sixty SFP ports are available for devices.

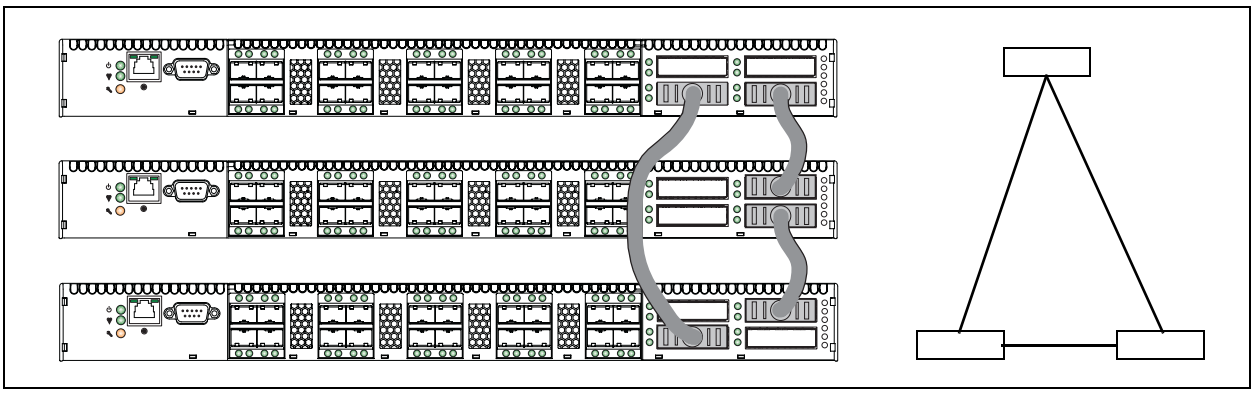


Figure 3-2 Three-Switch Stack

Figure 3-3 shows a four-switch stack of model 5802V switches using three 3-inch and three 9-inch XPAK switch stacking cables. Eighty SFP ports are available for devices.

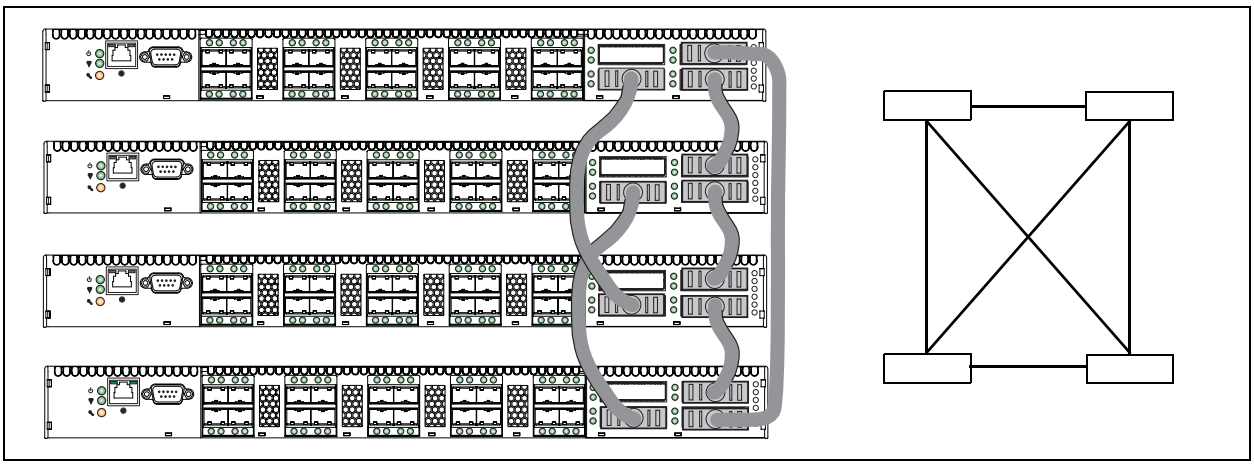


Figure 3-3 Four-Switch Stack

Figure 3-4 shows a five-switch stack of model 5802V switches using ten XPAK switch stacking cables. One hundred SFP ports are available for devices.

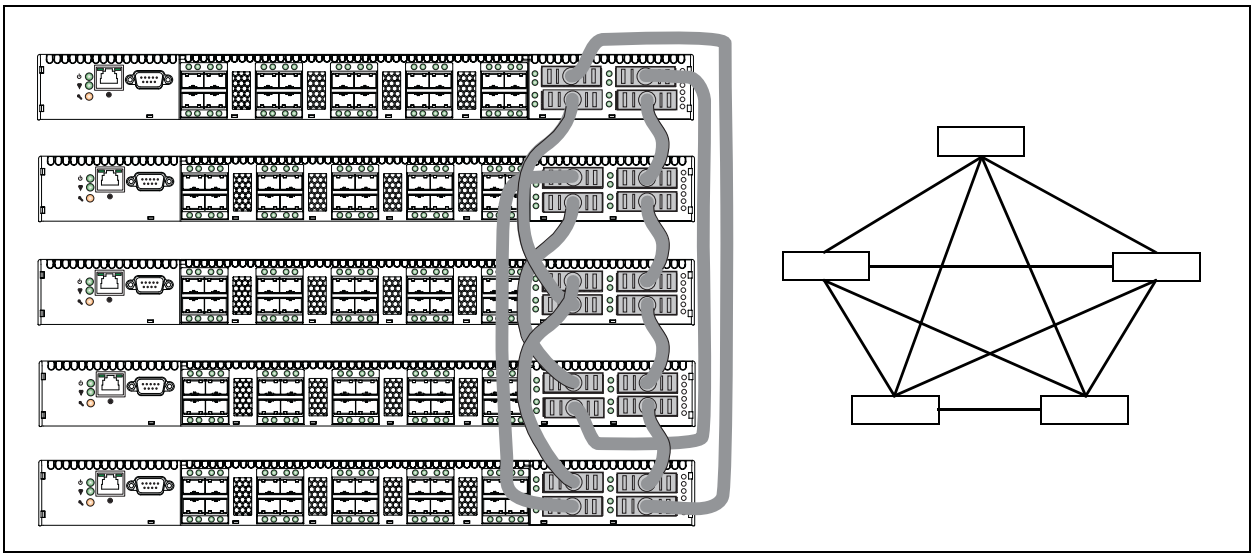


Figure 3-4 Five Switch Stack

Figure 3-5 shows a six-switch stack of model 5802V switches using eight XPAK switch stacking cables. One hundred twenty SFP ports are available for devices.

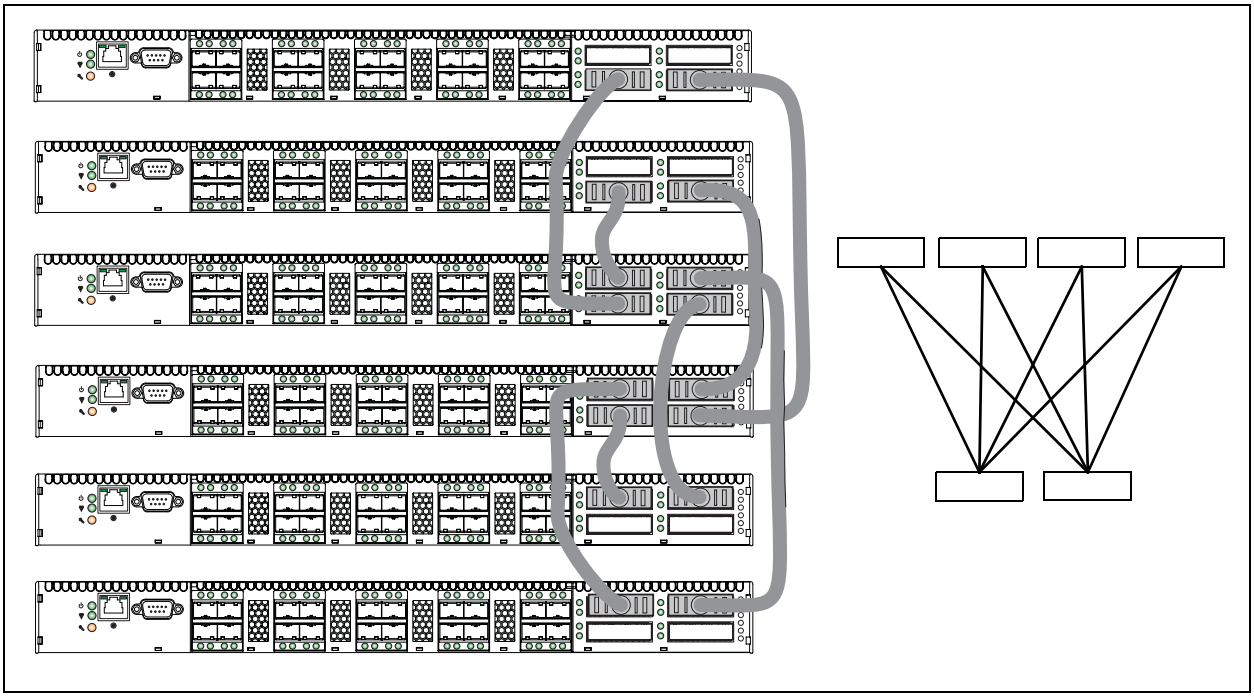


Figure 3-5 Six Switch Stack

Common Topologies

The SANbox 5802V switch supports the following topologies using the Fibre Channel SFP ports:

- Cascade Topology
- Mesh Topology
- MultiStage Topology

Cascade Topology

A cascade topology describes a fabric in which the switches are connected in series. If you connect the last switch back to the first switch, you create a cascade-with-a-loop topology as shown in Figure 3-6. The loop reduces latency because any switch can route traffic in the shortest direction to any switch in the loop. The loop also provides failover should a switch fail.

Using 20-port SANbox 5802V switches, the cascade fabric shown in Figure 3-6 has the following characteristics:

- Each chassis link contributes up to 850 MB of bandwidth between chassis, 1700 MB in full duplex. However, because of the sequential structure, that bandwidth will be shared by traffic between devices on other chassis.
- Latency between any two ports is no more than two chassis hops.
- Sixty-four Fibre Channel SFP ports are available for devices.

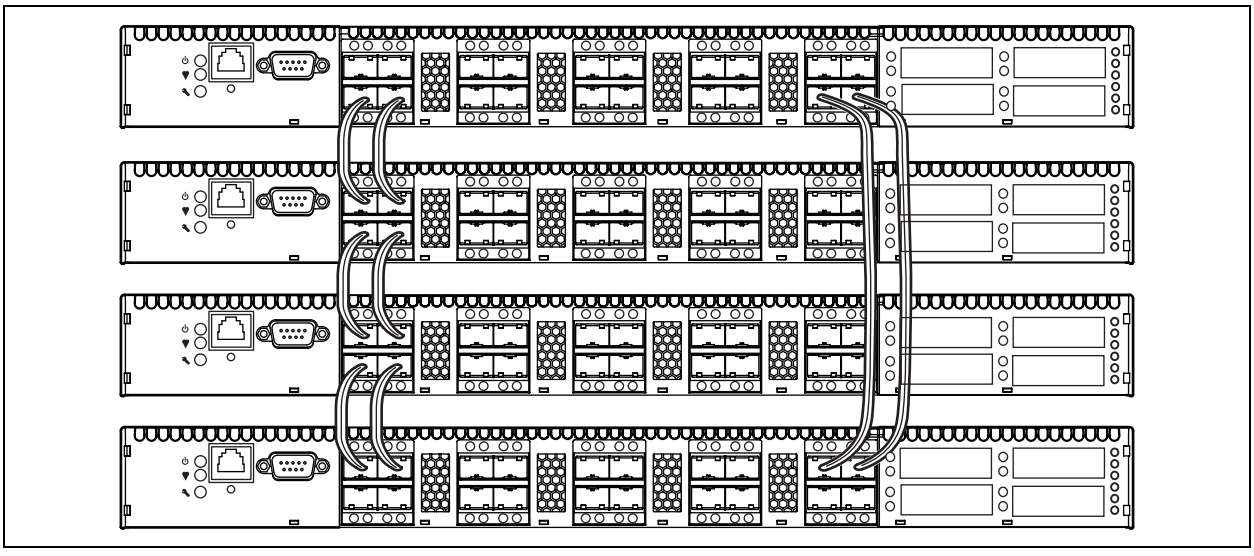


Figure 3-6 Cascade-with-a-Loop Topology

Mesh Topology

A mesh topology describes a fabric in which each chassis has at least one port directly connected to each other chassis in the fabric. Using 20-port SANbox 5802V switches the mesh fabric shown in Figure 3-7 has the following characteristics:

- Each link contributes up to 850 MB of bandwidth between switches, 1700 MB in full duplex. Because of multiple parallel paths, there is less competition for this bandwidth than with a cascade or a Multistage topology.
- Latency between any two ports is one chassis hop.
- Fifty-six Fibre Channel SFP ports are available for devices.

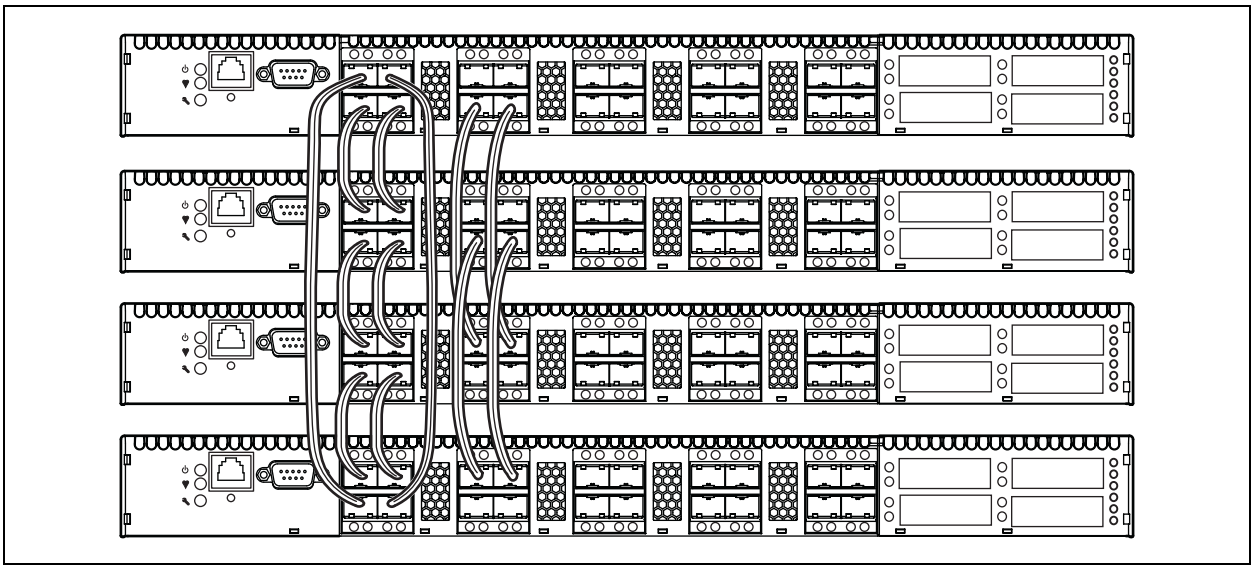


Figure 3-7 Mesh Topology

MultiStage Topology

A Multistage™ topology describes a fabric in which two or more edge switches connect to one or more core switches. Using 20-port SANbox 5802V switches, the Multistage fabric shown in Figure 3-8 has the following characteristics:

- Each link contributes up to 850 MB of bandwidth between chassis. Competition for this bandwidth is less than that of a cascade topology, but greater than that of the mesh topology.
- Latency between any two ports is no more than two chassis hops.
- Seventy-two Fibre Channel SFP ports are available for devices.

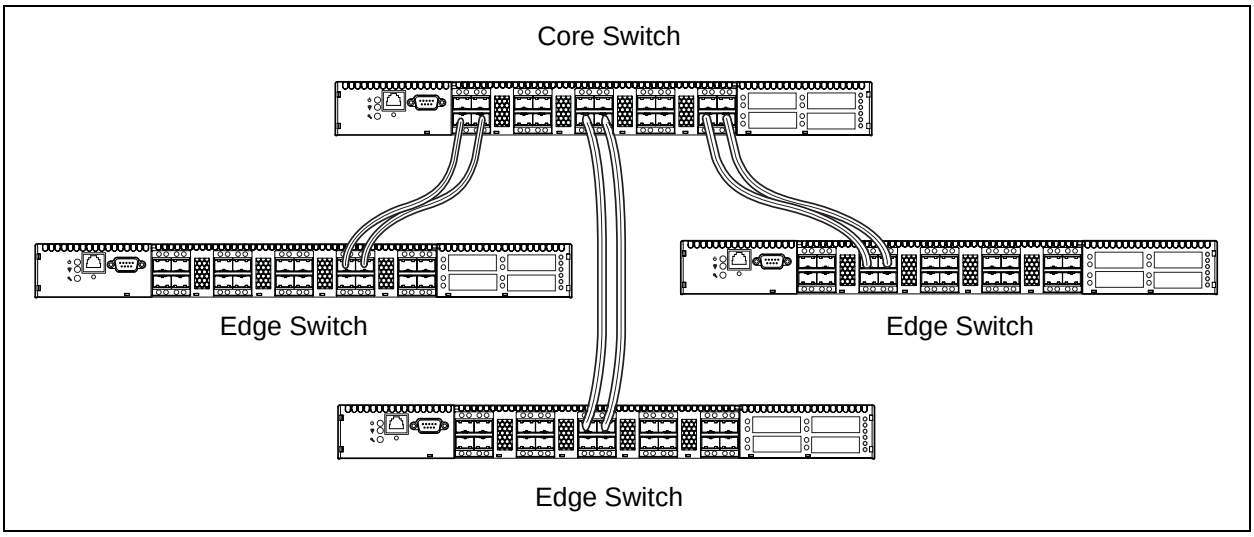


Figure 3-8 Multistage Topology

Switch Services

You can configure your switch to suit the demands of your environment by enabling or disabling a variety of switch services. Familiarize yourself with the following switch services and determine which ones you need. Notice that the SSH and SSL services require the Fabric Security license key.

- **Telnet**: Provides for the management of the switch over a Telnet connection. Disabling this service is not recommended. The default is enabled.
- **Secure Shell (SSH)**: Provides for secure remote connections to the switch using SSH. Your workstation must also use an SSH client. The default is disabled. This service requires the Fabric Security license key.
- **GUI Management**: Provides for out-of-band management of the switch with Enterprise Fabric Suite 2007, QuickTools, the Application Programming Interface (API), SNMP, and SMI-S. If this service is disabled, the switch can only be managed inband or through the serial port. The default is enabled.
- **Inband Management**: Provides for the management of the switch over an inter-switch link using Enterprise Fabric Suite 2007, QuickTools, SNMP, management server, or the API. If you disable inband management, you can no longer communicate with that switch by means other than an Ethernet or serial connection.The default is enabled.
- **Secure Socket Layer (SSL)**: Provides for secure SSL connections for Enterprise Fabric Suite 2007, the QuickTools web applet, the API, and SMI-S. This service must be enabled to authenticate users through a RADIUS server when using Enterprise Fabric Suite 2007. To enable secure SSL connections, you must first synchronize the date and time on the switch and workstation. Enabling SSL automatically creates a security certificate on the switch. The default is enabled. This service requires the Fabric Security license key.
- **QuickTools web applet (EmbeddedGUI)**: Provides for access to the QuickTools web applet. QuickTools enables you to point at a switch with an internet browser and manage the switch through the browser. The default is enabled.
- **Simple Network Management Protocol (SNMP)**: Provides for the management of the switch through third-party applications that use the Simple Network Management Protocol (SNMP). Security consists of a read community string and a write community string that serve as passwords that control read and write access to the switch. These strings are set at the factory to these well-known defaults and should be changed if SNMP is to be enabled. Otherwise, you risk unwanted access to the switch. The default is enabled.

- **Common Information Model (CIM)**: Provides for the management of the switch through third-party applications that use the Storage Management Initiative–Specification (SMI-S). The default is enabled.
- **File Transfer Protocol (FTP)**: Provides for transferring files rapidly between the workstation and the switch using FTP. The default is enabled.
- **Management Server (MS)**: Enables or disables the management of the switch through third-party applications that use GS-3 Management Server. The default is disabled.
- **Call Home:** Provides for automated e-mail notification of switch status and operating conditions based on specified event severity levels. The default is enabled. The Call Home service requires an Ethernet connection to at least one Simple Mail Transfer Protocol (SMTP) server. You must configure the Call Home service to do the following:
  - Enable primary and secondary SMTP servers and specify their IP addresses
  - Specify contact information

  Configure one or more Call Home profiles to specify mail recipients, message format, and the event severity level that will initiate a message.

Fabric Security

An effective security profile begins with a security policy that states the requirements. A threat analysis is needed to define the plan of action followed by an implementation that meets the security policy requirements. Internet portals, such as remote access and E-mail, usually present the greatest threats. Fabric security should also be considered in defining the security policy.

Most fabrics are located at a single site and are protected by physical security, such as key-code locked computer rooms. For these cases, security methods such as user passwords for equipment and zoning for controlling device access, are satisfactory.

Fabric security is needed when security policy requirements are more demanding: for example, when fabrics span multiple locations and traditional physical protection is insufficient to protect the IT infrastructure. Another benefit of fabric security is that it creates a structure that helps prevent unintended changes to the fabric.

Fabric security consists of the following:

- Connection Security
- User Account Security
- Port Binding
- Device Security

Connection Security

NOTE:

You must install the Fabric Security license key to secure connections using SSH and SSL.

Connection security provides an encrypted data path for switch management methods. The switch supports the Secure Shell (SSH) protocol for the command line interface and the Secure Socket Layer (SSL) protocol for management applications such as Enterprise Fabric Suite 2007 and SMI-S.

The SSL handshake process between the workstation and the switch involves the exchanging of certificates. These certificates contain the public and private keys that define the encryption. When the SSL service is enabled, a certificate is automatically created on the switch. The workstation validates the switch certificate by comparing the workstation date and time to the switch certificate creation date and time. For this reason, it is important to synchronize the workstation and switch with the same date, time, and time zone. The switch certificate is valid 24 hours before its creation date and 365 days after its creation date. If the certificate should become invalid, create a new certificate using the Create Certificate CLI command. Refer to the *SANbox 5802V Fibre Channel Switch Command Line Interface Guide* for information about the Create Certificate CLI command.

Consider your requirements for connection security: for the command line interface (SSH), management applications such as Enterprise Fabric Suite 2007 (SSL), or both. Access to the device security menu selections in Enterprise Fabric Suite 2007 requires an SSL connection. If an SSL connection security is required, also consider using the Network Time Protocol (NTP) to synchronize workstations and switches.

User Account Security

User account security consists of the administration of account names, passwords, expiration date, and authority level. If an account has Admin authority, all management tasks can be performed by that account in the CLI and QuickTools. Otherwise only monitoring tasks are available. The default account name, Admin, is the only account that can create or add account names and change passwords of other accounts. All users can change their own passwords. Account names and passwords are always required when connecting to a switch.

Authentication of the user account and password can be performed locally using the switch's user account database or it can be done remotely using a RADIUS server such as Microsoft® RADIUS. Authenticating user logins on a RADIUS server requires a secure management connection to the switch. Refer to "Connection Security" on page 3-16 for information about securing the management connection. A RADIUS server can also be used to authenticate devices and other switches as described in "Device Security" on page 3-18.

Consider your management needs and determine the number of user accounts, their authority needs, and expiration dates. Also consider the advantages of centralizing user administration and authentication on a RADIUS server.

NOTE:

If the same user account exists on a switch and its RADIUS server, that user can login with either password, but the authority and account expiration will always come from the switch database.

Port Binding

Port binding provides authorization for a list of up to 32 switch and device WWNs that are permitted to log in to a particular switch port. Switches or devices that are not among the 32 are refused access to the port. Consider what ports to secure and the set of switches and devices that are permitted to log in to those ports. For information about port binding, refer to the *SANbox 5802V Fibre Channel Switch Command Line Interface Guide*.

Device Security

NOTE:

You must install the Fabric Security license key to configure and activate device security and RADIUS servers.

Device security provides for the authorization and authentication of devices that you attach to a switch. You can configure a switch with a group of devices against which the switch authorizes new attachments by devices, other switches, or devices issuing management server commands. Device security is configured through the use of security sets and groups.

A group is a list of device worldwide names that are authorized to attach to a switch. There are three types of groups: one for other switches (ISL), another for devices (port), and a third for devices issuing management server commands (MS).

A security set is a set of up to three groups with no more than one of each group type. The security configuration is made up of all security sets on the switch. The security database has the following limits:

- Maximum number of security sets is 4.
- Maximum number of groups is 16.
- Maximum number of members in a group is 1000.
- Maximum total number of group members is 1000.

In addition to authorization, the switch can be configured to require authentication to validate the identity of the connecting switch, device, or host. Authentication can be performed locally using the switch's security database, or remotely using a Remote Dial-In User Service (RADIUS) server such as Microsoft® RADIUS. With a RADIUS server, the security database for the entire fabric resides on the server. In this way, the security database can be managed centrally, rather than on each switch. You can configure up to five RADIUS servers to provide failover.

You can configure the RADIUS server to authenticate just the switch or both the switch and the initiator device if the device supports authentication. When using a RADIUS server, every switch in the fabric must have a network connection. A RADIUS server can also be configured to authenticate user accounts as described in "User Account Security" on page 3-17. A secure connection is required to authenticate user logins with a RADIUS server. Refer to "Connection Security" on page 3-16 for more information.

Consider the devices, switches, and management agents and evaluate the need for authorization and authentication. Also consider whether the security database is to distributed on the switches or centralized on a RADIUS server and how many servers to configure.

The following examples illustrate how to configure a security database:

- Security Example: Switches and HBAs with Authentication
- Security Example: RADIUS Server
- Security Example: Host Authentication

Security Example: Switches and HBAs with Authentication

Consider the fabric shown in Figure 3-9. In this fabric, Switch_1, HBA_1, and Switch_2 support authentication while the JBOD and HBA_2 do not. The objective is to secure F_Ports and E_Ports in the fabric. To do this, configure security on the devices that support security: Switch_1, Switch_2, and HBA_1.

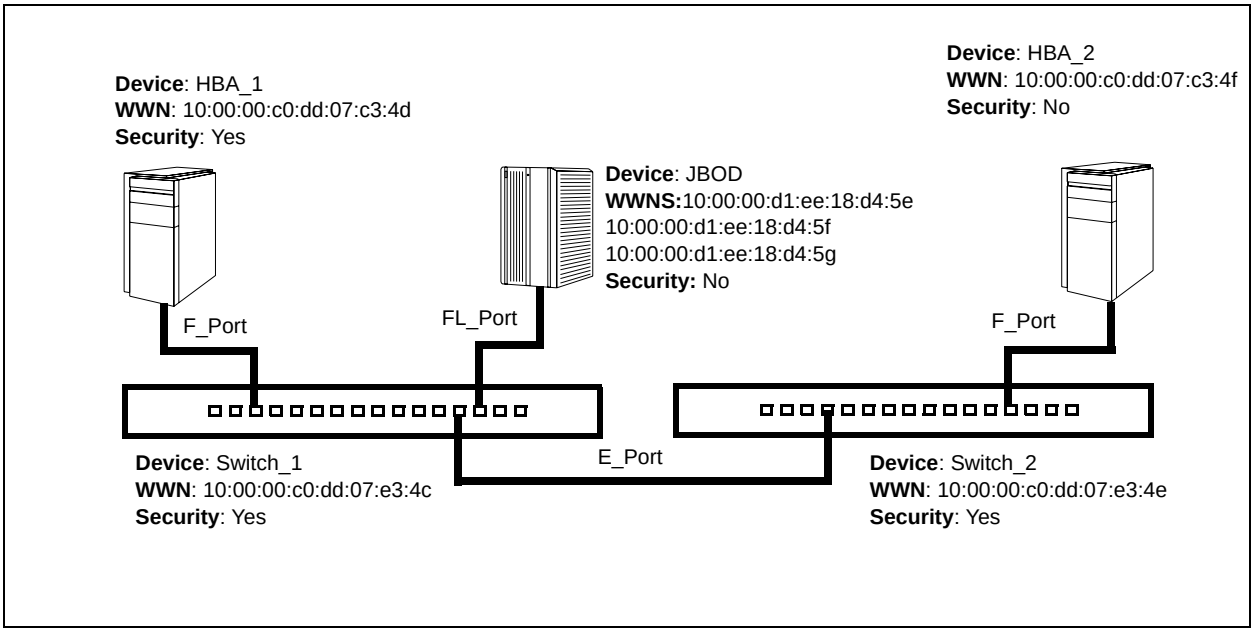


Figure 3-9 Security Example: Switches and HBAs

1. Create a security set (Security_Set_1) on Switch_1.
   a. Create a port group (Group_Port_1) in Security_Set_1 with Switch_1, HBA_1, and JBOD as members.

Switch_1	Node WWN: 10:00:00:c0:dd:07:e3:4c Authentication: CHAP Primary Hash: MD5 Primary Secret: 0123456789abcdef
HBA_1	Node WWN: 10:00:00:c0:dd:07:c3:4d Authentication: CHAP Primary Hash: MD5 Primary Secret: fedcba9876543210
JBOD	Node WWN: 10:00:00:d1:ee:18:d4:5e Authentication: None Node WWN: 10:00:00:d1:ee:18:d4:5f Authentication: None Node WWN: 10:00:00:d1:ee:18:d4:5g Authentication: None

   - Switch_1 and all devices and switches connected to Switch_1 must be included in the group even if the switch or devices does not support authentication. Others wise, the Switch_1 port will isolate.
   - You must specify HBAs by node worldwide name. Switches can be specified by port or node worldwide name. The type of switch worldwide name you use in the switch security database must be the same as that in the HBA security database. For example, if you specify a switch with a port worldwide name in the switch security database, you must also specify that switch in the HBA security database with the same port worldwide name.
   - For CHAP authentication, create 32-character hexadecimal or 16-character ASCI secrets. The switch secret must be shared with the HBA security database.

b. Create an ISL group (Group_ISL_1) in Security_Set_1 with Switch_1, Switch_2, HBA1, and JBOD as members. The Switch_1 secret must be shared with the Switch_2 security database.

Switch_1	Node WWN: 10:00:00:c0:dd:07:e3:4c Authentication: CHAP Primary Hash: MD5 Primary Secret: 0123456789abcdef Binding: None
Switch_2	Node WWN: 10:00:00:c0:dd:07:e3:4e Authentication: CHAP Primary Hash: MD5 Primary Secret: abcdefabcdef012 Binding: None

2. Configure security on HBA_1 using the appropriate management tool. Logins between the Switch_1 and HBA_1 will be challenged for their respective secrets. Therefore, the secrets for Switch_1 and HBA_1 that you configured on Switch_1 must also be configured on HBA_1.
3. Save and activate Security_Set_1 on Switch_1.
4. Create a security set (Security_Set_2) on Switch_2. Create an ISL group (Group_ISL_2) in Security_Set_2 with Switch_2 and Switch_1 as members.

Switch_2	Node WWN: 10:00:00:c0:dd:07:e3:4e Authentication: CHAP Primary Hash: MD5 Primary Secret: 0123456789abcdef Binding: None
Switch_1	Node WWN: 10:00:00:c0:dd:07:e3:4c Authentication: CHAP Primary Hash: MD5 Secret: abcdefabcdef012 Binding: None

5. Save and activate Security_Set_2 on Switch_2.

Security Example: RADIUS Server

Consider the fabric shown in Figure 3-10. This fabric is similar to the one shown in Figure 3-9 with the addition of Radius_1 acting as a RADIUS server. Authorization and authentication is passed from the switch to Radius_1 in the following cases:

- HBA_1 login to Switch_1
- Switch_1 login to Switch_2
- Switch_2 login to Switch_1

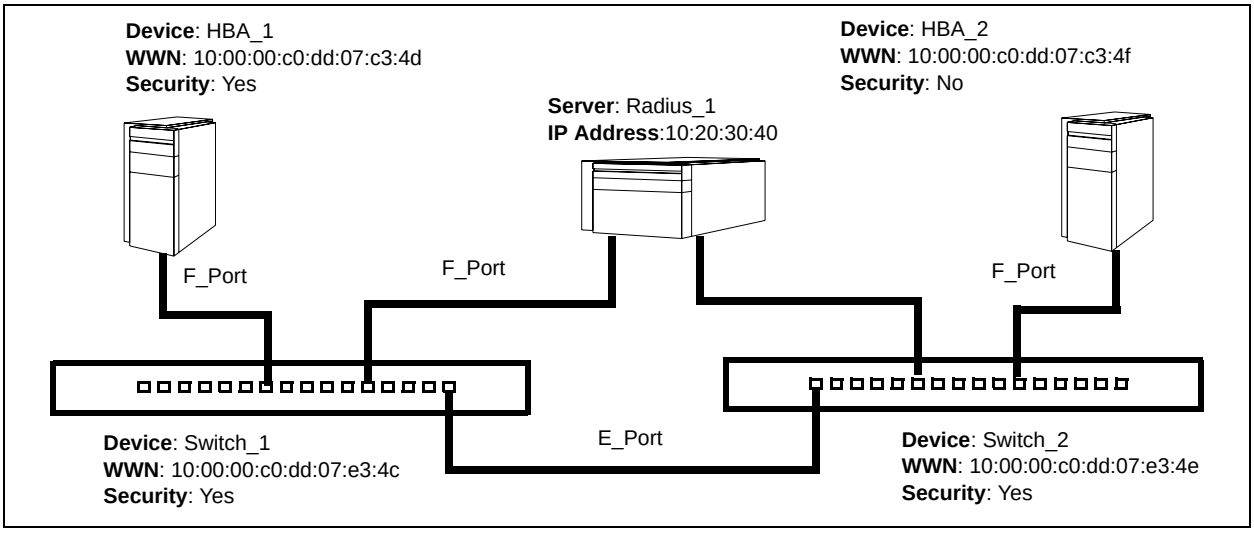


Figure 3-10 Security Example: RADIUS Server

1. Configure the Radius_1 host as a RADIUS server on Switch_1 and Switch_2 to authenticate device logins. Specify the server IP address and the secret with which the switches will authenticate with the server. Configure the switches so that devices authenticate through the switches only if the RADIUS server is unavailable.

Device Authentication Order	RadiusLocal – Authenticate devices using the RADIUS server security database first. If the RADIUS server is unavailable, then use the local switch security database.
Total Servers	1 – Enables support for one RADIUS server
Device Authentication Server	True – Enables Radius_1 to authenticate device logins.
Server IP Address	10.20.30.40
Secret	1234567890123456 – 16-character ASCI string (MD5 hash). This is the secret that allows direct communication with the RADIUS server.

2. Create a security set (Security_Set_1) on Switch_1.

   a. Create a port group (Group_Port_1) in Security_Set_1 with Switch_1 and HBA_1 as members.

Switch_1	Node WWN: 10:00:00:c0:dd:07:e3:4c Authentication: CHAP Primary Hash: MD5 Primary Secret: 0123456789abcdef
HBA_1	Node WWN: 10:00:00:c0:dd:07:c3:4d Authentication: CHAP Primary Hash: MD5 Primary Secret: fedcba9876543210

   - Switch_1 and all devices and switches connected to Switch_1 must be included in the group even if the switch or device does not support authentication. Others wise, the Switch_1 port will isolate.
   - You must specify HBAs by node worldwide name. Switches can be specified by port or node worldwide name. The type of switch worldwide name you use in the switch security database must be the same as that in the HBA security database. For example, if you specify a switch with a port worldwide name in the switch security database, you must also specify that switch in the HBA security database with the same port worldwide name.
   - For CHAP authentication, create 32-character hexadecimal or 16-character ASCI secrets. The switch secret must be shared with the HBA security database.

b. Create an ISL group (Group_ISL_1) in Security_Set_1 with Switch_1 and Switch_2 as members. The Switch_1 secret must be shared with the Switch_2 security database.

Switch_1	Node WWN: 10:00:00:c0:dd:07:e3:4c Authentication: CHAP Primary Hash: MD5 Primary Secret: 0123456789abcdef Binding: None
Switch_2	Node WWN: 10:00:00:c0:dd:07:e3:4e Authentication: CHAP Primary Hash: MD5 Primary Secret: abcdefabcdef012 Binding: None

3. Configure security on HBA_1 using the appropriate management tool. Logins between the Switch_1 and HBA_1 will be challenged (CHAP) for their respective secrets. Therefore, the secrets for Switch_1 and HBA_1 that you configured on Switch_1 must also be configured on HBA_1.
4. Save and activate Security_Set_1 on Switch_1.
5. Create a security set (Security_Set_2) on Switch_2. Create an ISL group (Group_ISL_2) in Security_Set_2 with Switch_1 and Switch_2 as members.

Switch_2	Node WWN: 10:00:00:c0:dd:07:e3:4e Authentication: CHAP Primary Hash: MD5 Primary Secret: abcdefabcdef0123 Binding: None
Switch_1	Node WWN: 10:00:00:c0:dd:07:e3:4c Authentication: CHAP Primary Hash: MD5 Primary Secret: 0123456789abcdef Binding: None

6. Save and activate Security_Set_2 on Switch_2.

Security Example: Host Authentication

Consider the fabric shown in Figure 3-11. In this fabric, only Switch_2 and HBA_2/APP_2 support security, where APP_2 is a host application. The objective is to secure the management server on Switch_2 from unauthorized access by an HBA or an associated host application.

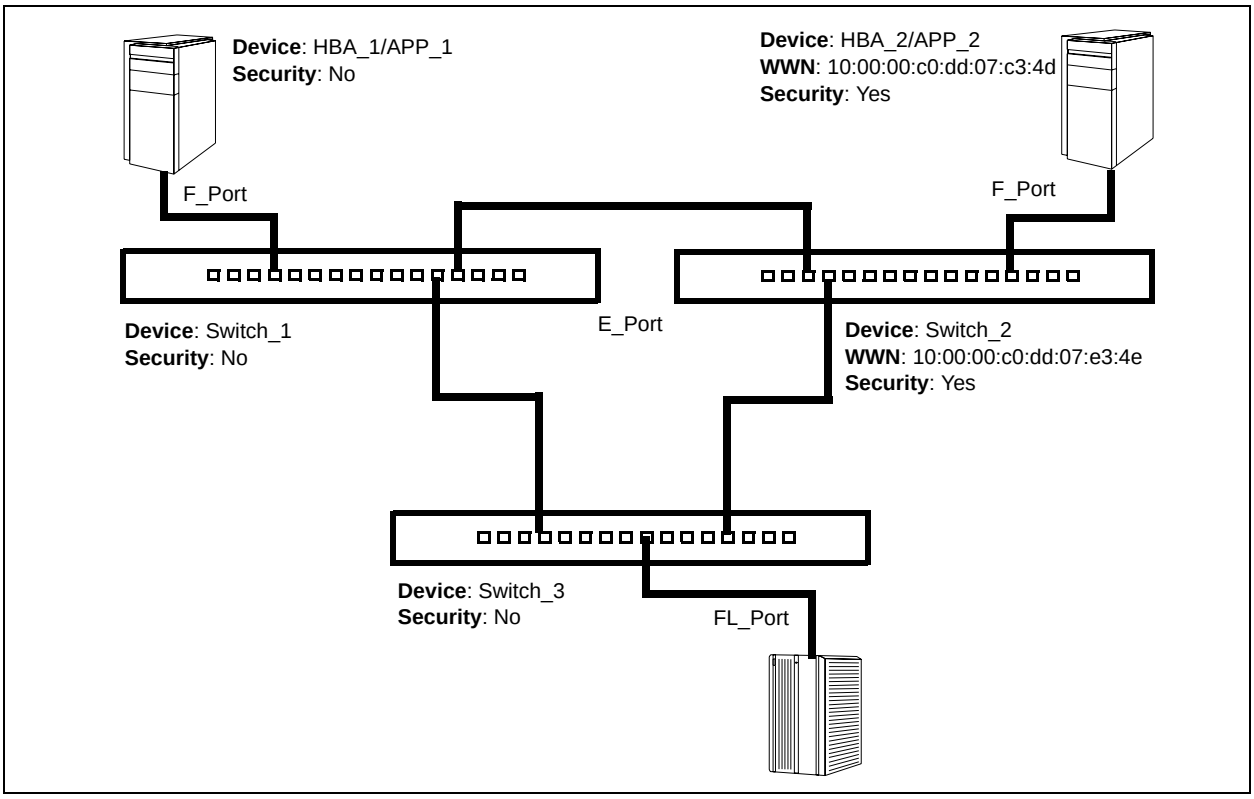


Figure 3-11 Security Example: Management Server

1. Create a security set (Security_Set_2) on Switch_2.
2. Create a Management Server group (Group_1) in Security_Set_2 with Switch_2 and HBA_2 or APP_2 as its member.
   - You must specify HBAs by node worldwide name. Switches can be specified by port or node worldwide name. The type of switch worldwide name you use in the switch security database must be the same as that in the HBA security database. For example, if you specify a switch with a port worldwide name in the switch security database, you must also specify that switch in the HBA security database with the same port worldwide name.
   - For MD5 authentication, create secrets.

Switch_2	Node WWN: 10:00:00:c0:dd:07:c3:4e CT Authentication: True Hash: MD5 Secret: 9876543210fedcba9
HBA_2 or APP_2	Node WWN: 10:00:00:c0:dd:07:c3:4d CT Authentication: True Hash: MD5 Secret: fedcba9876543210

3. Configure security on HBA_2 or APP_2 using the appropriate management tool. Logins between the Switch_2 and HBA_2 or APP_2 will be challenged (MD5) for their respective secrets. Therefore, the secrets that you configured for HBA_2 or APP_2 on Switch_2 must also be configured on HBA_2 or APP_2.
4. Save and activate Security_Set_2.

Fabric Management

The browser-based application, QuickTools, and the CLI reside in the switch firmware and provide for the management of individual switches in a single fabric. Consider how many fabrics and switches will be managed, how many management workstations are needed, and whether the fabrics will be managed with QuickTools or the CLI.

A switch supports a combined maximum of 19 logins that are reserved as follows:

- 4 logins or sessions for internal applications such as management server and SNMP
- 9 high priority Telnet sessions
- 6 logins or sessions for Enterprise Fabric Suite 2007 logins, QuickTools logins, Application Programming Interface (API) logins, and Telnet logins.

Additional logins will be refused.

4 Installation

This section describes how to install and configure the switch. The following topics are covered:

- Site Requirements
- Installing a Switch
- Installing Firmware
- Adding a Switch to an Existing Fabric
- Installing Feature License Keys

Site Requirements

Consider the following items when installing a SANbox 5802V switch:

- Fabric Management Workstation
- Switch Power Requirements
- Environmental Conditions

Fabric Management Workstation

The requirements for fabric management workstations are described in Table 4-1:

Table 4-1. Management Workstation Requirements

Operating System	■ Windows 2003 and XP SP1/SP2 ■ Solaris 9, 10, 10 x86 ■ Red Hat® Enterprise Linux® 3, 4 ■ SUSE™ Linux Enterprise Server 9, 10 ■ Mac® OS X 10.4
Memory	256 MB or more; 512 MB recommended
Processor	1 GHz or faster
Internet Browser	Microsoft® Internet Explorer® 6.0 or later Netscape Navigator® 6.0 and later Mozilla™ 1.5 and later Safari® 1.0 and later Firefox 1.0 and later Java 2 Standard Edition Runtime Environment 1.4.2 for QuickTools

Telnet workstations require an RJ-45 Ethernet port or an RS-232 serial port and an operating system with a Telnet client.

Switch Power Requirements

Power requirements are 1 Amp at 100 VAC or 0.5 A at 240 VAC.

Environmental Conditions

Consider the factors that affect the climate in your facility such as equipment heat dissipation and ventilation. The switch requires the following operating conditions:

- Operating temperature range: 5–40°C (41–104°F)
- Relative humidity: 10–90%, non-condensing

Installing a Switch

Unpack the switch and accessories. The SANbox 5802V product is shipped with the components shown in Figure 4-1:

- SANbox 5802V Fibre Channel (1) with firmware installed
- Power cords (2)
- Rubber feet (4)

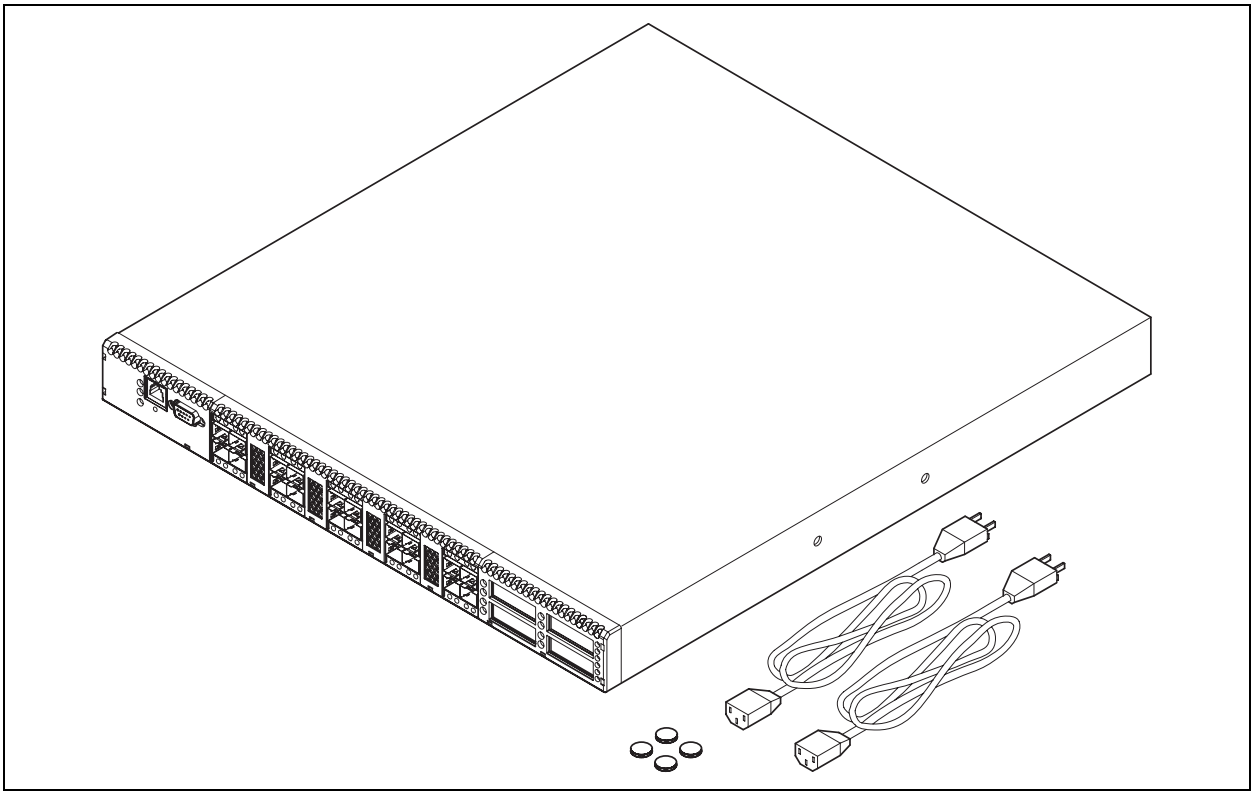


Figure 4-1 SANbox 5802V Fibre Channel

Installing a SANbox 5802V switch involves the following steps:

1. Mount the Switch
2. Install Transceivers
3. Configure the Workstation
4. Connect the Switch to AC Power
5. Connect the Workstation to the Switch
6. Configure the Switch
7. Cable Devices to the Switch

Mount the Switch

The switch can be placed on a flat surface and stacked, or mounted in a 19” Electronics Industries Association (EIA) rack. Refer to “Dimensions” on page A-5 for weight and dimensional specifications. Adhesive rubber feet are provided for surface mounts. Without the rubber feet, the switch occupies 1U of space in an EIA rack. Rack mounting requires a QLogic rail kit (part number SB-RACKKIT).

WARNING!!

Mount switches in the rack so that the weight is distributed evenly. An unevenly loaded rack can become unstable possibly resulting in equipment damage or personal injury.

AVERTISSEMENT!!

Installer les commutateurs dans l’armoire informatique de sorte que le poids soit réparti uniformément. Une armoire informatique déséquilibré risque d'entraîner des blessures ou d'endommager l'équipement.

WARNUNG!!

Switches so in das Rack einbauen, dass das Gewicht gleichmäßig verteilt ist. Ein Rack mit ungleichmäßiger Gewichtsverteilung kann schwanken/umfallen und Gerätbeschädigung oder Verletzung verursachen

¡ADVERTENCIA!

Monte los conmutadores en el estante de modo que el peso se distribuya de manera uniforme. Un estante cuya carga no esté distribuida de manera uniforme puede ser inestable y podría dañar el equipo o causar lesiones personales.

CAUTION!

- If the switch is mounted in a closed or multi-rack assembly, the operating temperature of the rack environment may be greater than the ambient temperature. Be sure to install the chassis in an environment that is compatible with the maximum rated ambient temperature. Refer to "Environmental" on page A-7 for technical specifications.
- Do not restrict chassis air flow. Allow 16 cm (6.5 in) minimum clearance at the front and rear of the switch (surface mount) or rack for service access and ventilation.
- Multiple rack-mounted units connected to the AC supply circuit may overload that circuit or overload the AC supply wiring. Consider the power source capacity and the total power usage of all switches on the circuit. Refer to "Electrical" on page A-5.
- Reliable grounding in the rack must be maintained from the switch chassis to the AC power source.

Install Transceivers

The switch supports a variety of SFP and XPAK transceivers. To install a transceiver, insert the transceiver into the port and gently press until it snaps in place. To remove a transceiver, gently press the transceiver into the port to release the tension, then pull on the release tab or lever and remove the transceiver. Different transceiver manufacturers have different release mechanisms. Consult the documentation for your transceiver.

NOTE:

The transceiver will fit only one way. If the transceiver does not install under gentle pressure, flip it over and try again.

CAUTION!

To maintain proper air flow and prevent the switch from overheating, keep covers installed in unused XPAK ports.

If you are using the XPAK ports, remove the port covers by the cover tabs using your fingers or pliers as shown in Figure 4-2.

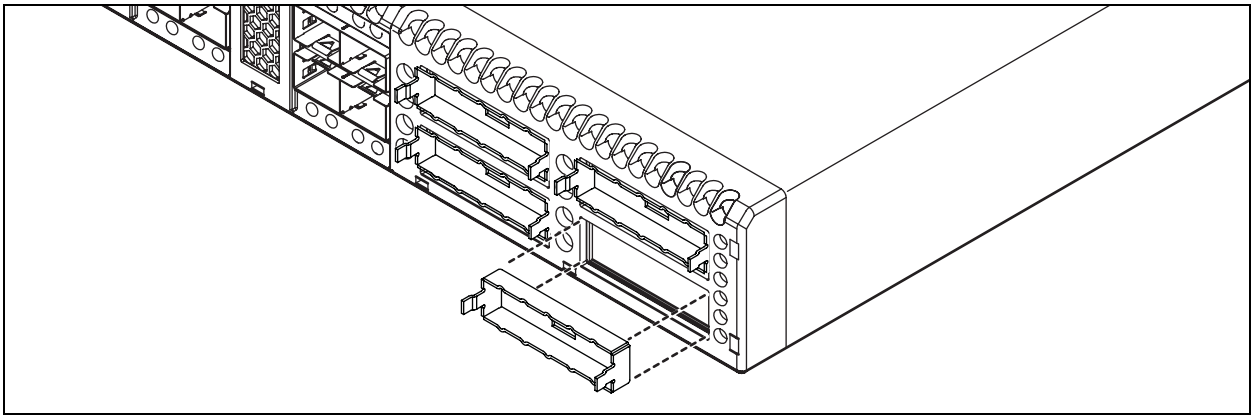


Figure 4-2 Removing XPAK Port Covers

To install XPAK switch stacking cables, position the cable connectors with the circuit board toward the mid line of the respective switch faceplates as shown in Figure 4-3. When installing the 3-inch XPAK switch stacking cable, insert the cable connectors into the XPAK ports at the same time.

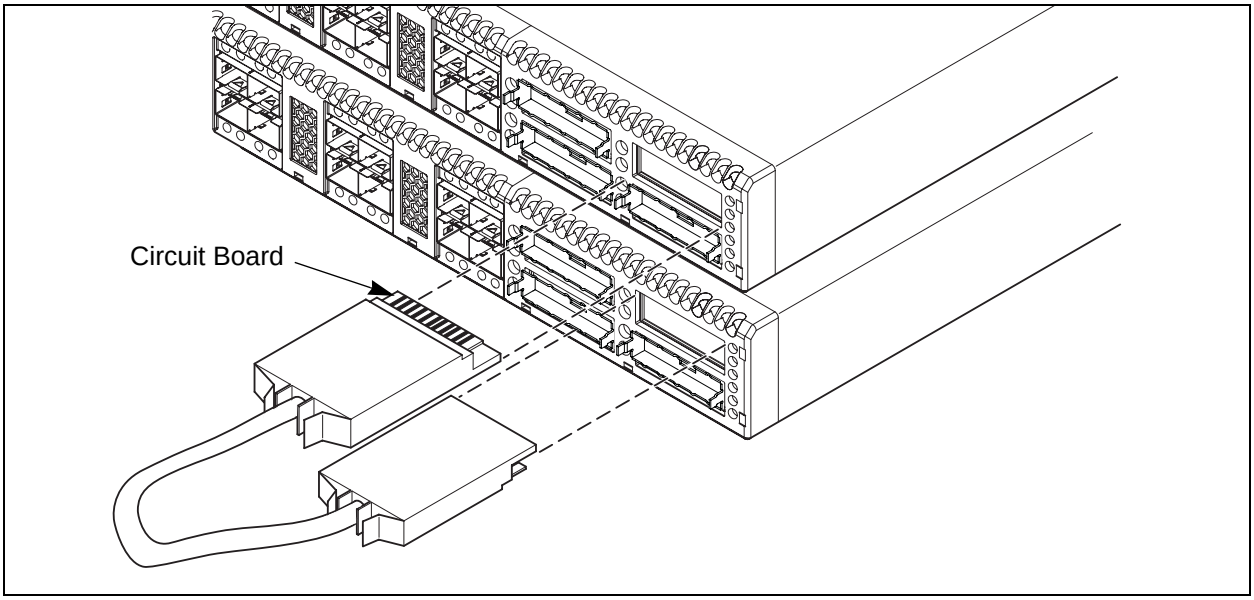


Figure 4-3 Installing XPAK Switch Stacking Cables

Configure the Workstation

NOTE:

If you plan to use QuickTools to manage the switch, the Configuration Wizard manages the workstation IP address for you – proceed to “Connect the Workstation to the Switch” on page 4-12.

If you plan to use the CLI to configure and manage the switch, you must configure the workstation. This involves setting the workstation IP address for Ethernet connections, or configuring the workstation serial port.

Configuring the Workstation IP Address for Ethernet Connections

The default IP address of a new switch is 10.0.0.1. To ensure that your workstation is configured to communicate with the 10.0.0 subnet, refer to the following instructions for your workstation:

- For a Windows workstation, do the following:
  1. Click the **Start** button and choose **Settings**>**Control Panel**>**Network and Dial-Up Connections**.
  2. Choose **Make New Connection**.
  3. Click the **Connect to a private network through the Internet** radio button then click the **Next** button.
  4. Enter 10.0.0.253 for the IP address.
- For a Linux or Solaris workstation, open a command window and enter the following command where (interface) is your interface name:

```
ifconfig (interface) ipaddress 10.0.0.253 netmask 255.255.255.0 up
```

- For a MacOS X workstation, do the following:
  1. Choose **System Preferences>System Preferences>Network**.
  2. Double-click your network adapter.
  3. In the configuration dialog, select **Manually** from the Configure IPv4 drop down menu.
  4. Enter 10.0.0.253 in the IP Address field.
  5. Enter 255.255.255.0 in the Subnet Mask field.
  6. Click **Apply Now**.

Configuring the Workstation Serial Port

To configure the workstation serial port, do the following:

1. Connect a null modem F/F DB9 cable from a COM port on the management workstation to the RS-232 serial port on the switch.
2. Configure the workstation serial port according to your platform:
   - For Windows:
     a. Open the HyperTerminal application. Choose the **Start** button, select **Programs, Accessories, HyperTerminal,** and **HyperTerminal**.
     b. Enter a name for the switch connection and choose an icon in the Connection Description window. Choose the **OK** button.
     c. Enter the following COM Port settings in the COM Properties window and choose the **OK** button.
        - ❑ Bits per second: 9600
        - ❑ Data Bits: 8
        - ❑ Parity: None
        - ❑ Stop Bits: 1
        - ❑ Flow Control: None
   - For Linux:
     a. Set up minicom to use the serial port. Create or modify the /etc/minirc.dfl file with the following content.

```
pr portdev/ttyS0
pu minit
pu mreset
pu mhangup
```

     b. Verify that all users have permission to run minicom. Review the /etc/minicom.users file and confirm that the line `ALL` exists or that there are specific user entries.
   - For Solaris: Modify the /etc/remote file to include the following lines. /dev/term/a refers to serial port a. Choose the "dv" setting to match the workstation port to which you connected to the switch.

```
hardwire:\:dv=/dev/term/a:br#9600:el=^C^S^Q^U^D:ie=%$:oe=^D:
```

3. Proceed to “Connect the Switch to AC Power” on page 4-9.

Connect the Switch to AC Power

WARNING!!

This product is supplied with a 3-wire power cable and plug for the user's safety. Use this power cable in conjunction with a properly grounded outlet to avoid electrical shock. An electrical outlet that is not correctly wired could place hazardous voltage on metal parts of the switch chassis. It is the responsibility of the customer to ensure that the outlet is correctly wired and grounded to prevent electrical shock.

You may require a different power cable in some countries because the plug on the cable supplied with the equipment will not fit your electrical outlet. In this case, you must supply your own power cable. The cable you use must meet the following requirements:

- For 125 Volt electrical service, the cable must be rated at 10 Amps and be approved by UL and CSA.
- For 250 Volt electrical service: The cable must be rated at 10 Amps, meet the requirements of H05VV-F, and be approved by VDE, SEMKO, and DEMKO.

AVERTISSEMENT!!

Pour la sécurité de l'utilisateur, l'appareil est livré avec un câble d'alimentation trifilaire et une fiche. Pour éviter toute secousse électrique, enficher ce câble à une prise correctement mise à la terre.Une prise électrique dont les fils sont mal branchés peut créer une tension dangereuse dans les pièces métalliques du châssis switch. Pour éviter toute secousse électrique, s'assurer que les fils sont correctement branchés et que la prise est bien mise à la terre.

Dans certains pays les prises électriques sont de modèle différent; on ne peut y enficher le câble de l'appareil. On doit donc en utiliser un autre ayant les caractéristiques suivantes:

- Alimentation 125 V: Câble pour courant nominal de 10 A, agréé LAC et CSA.
- Alimentation 250 V: Câble pour courant nominal de 10 A, conforme au H05VV-F, et agréé VDE, SEMKO et DEMKO.

WARNUNG!!

Dieses Produkt wird mit einem 3-adrigen Netzkabel mit Stecker geliefert. Dieses Kabel erfüllt die Sicherheitsanforderungen und sollte an einer vorschriftsmäßigen Schukosteckdose angeschlossen werden, um die Gefahr eines elektrischen Schlages zu vermeiden.Elektrosteckdosen, die nicht richtig verdrahtet sind, können gefährliche Hochspannung an den Metallteilen des switch-Gehäuses verursachen. Der Kunde trägt die Verantwortung für eine vorschriftsmäßige Verdrahtung und Erdung der Steckdose zur Vermeidung eines elektrischen Schlages.

In manchen Ländern ist eventuell die Verwendung eines anderen Kabels erforderlich, da der Stecker des mitgelieferten Kabels nicht in die landesüblichen Steckdosen paßt. In diesem Fall müssen Sie sich ein Kabel besorgen, daß die folgenden Anforderungen erfüllt:

- Für 125 Volt-Netze: 10 Ampere Kabel mit UL- und CSA-Zulassung.
- Für 250 Volt-Netze: 10 Ampere Kabel gemäß den Anforderungen der H05VV-F und VDE-, SEMKO- und DEMKO-Zulassung.

¡ADVERTENCIA!

Para garantizar la seguridad del usuario, este producto se suministra con un cable de alimentación de 3 hilos y un enchufe. Utilice este cable de alimentación junto con un enchufe correctamente conectado a tierra para evitar descargas eléctricas. Un enchufe eléctrico que no esté correctamente conectado puede hacer que las piezas metálicas del chasis del conmutador tengan un voltaje peligroso. Es responsabilidad del cliente asegurarse de que el enchufe esté correctamente conectado a una toma de tierra para evitar descargas eléctricas.

Es posible que en algunos países necesite un cable de alimentación diferente porque el enchufe del cable suministrado con el equipo no se ajusta a su enchufe eléctrico. En este caso, debe proveerse de su propio cable de alimentación. El cable que utilice debe cumplir los siguientes requisitos:

- Para un servicio eléctrico de 125 voltios, el cable debe tener una corriente nominal de 10 amperios y estar aprobado por UL y CSA.
- Para un servicio eléctrico de 250 voltios, el cable debe tener una corriente nominal de 10 amperios, cumplir los requisitos de H05VV-F y estar aprobado por VDE, SEMKO y DEMKO.

The switch comes with one or two NEMA 5-15, non-locking, power cords (SKU: CPK-5000-US). This power cord is approved for North America (USA, Canada, Puerto Rico), Mexico, Central America, South America, Korea, Taiwan, Philippines, and Thailand. Refer to Table A-6 for information about power cords for other regions/countries.

To power up the switch, connect the power cords to the power supply receptacles on the back of the switch chassis and to a grounded AC outlet. To provide redundancy in the event of an AC power circuit failure, connect the switch power supplies to separate AC circuits. The switch responds in the following sequence:

1. The chassis LEDs (Input Power, Heartbeat, System Fault) illuminate followed by all port Logged-In LEDs.
2. After a couple seconds the System Fault LED is extinguished while the Input Power LED and Heartbeat LED remain illuminated.
3. After approximately one minute, the POST executes and the Heartbeat LED is extinguished.
4. After about another minute, the POST is complete, all LEDs are extinguished except the Input Power LED and the Heartbeat LED:
   - The Input Power LED remains illuminated indicating that the switch logic circuitry is receiving DC voltage. If not, contact your authorized maintenance provider.
   - The Heartbeat LED indicates the results of the POST. The POST tests the condition of firmware, memories, data-paths, and switch logic circuitry. If the Heartbeat LED blinks steadily about once per second, the POST was successful, and you can continue with the installation process. Any other blink pattern indicates that an error has occurred. Refer to “Heartbeat LED Blink Patterns” on page 5-3 for more information about error blink patterns.

Connect the Workstation to the Switch

You can manage the switch using the CLI or QuickTools. QuickTools and requires an Ethernet connection to the switch. The CLI can use an Ethernet connection or a serial connection. Choose a switch management method, then connect the management workstation to the switch in one of the following ways:

- Indirect Ethernet connection from the management workstation to the switch RJ-45 Ethernet connector through an Ethernet switch or a hub. This requires a 10/100 Base-T straight cable as shown in Figure 4-4.
- Direct Ethernet connection from the management workstation to the switch RJ-45 Ethernet connector. This requires a 10/100 Base-T cross-over cable as shown in Figure 4-4.
- Serial port connection from the management workstation to the switch RS-232 serial port connector. This requires a null modem F/F DB9 cable as shown in Figure 4-4.

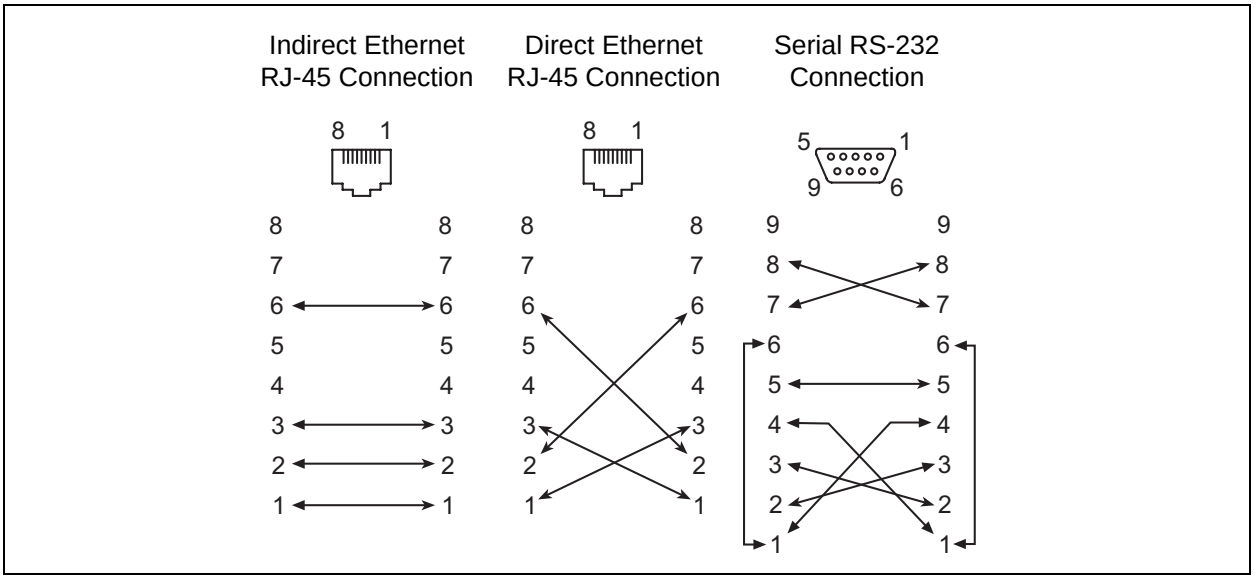


Figure 4-4 Workstation Cable Connections

Configure the Switch

You can configure the switch using the CLI or QuickTools.

QuickTools Switch Configuration

To log in and configure the switch using QuickTools, do the following:

1. Open an Internet browser and enter the default IP address 10.0.0.1 to start the QuickTools web applet.
2. Log in to the switch using the default user name (*admin*) and password (*password*).
3. Obtain the IP address and subnet mask from your network administrator.
4. Open the QuickTools Wizards menu and select **Configuration Wizard**. Follow the instructions to set the switch IP address and the password. Changing the IP address will terminate the QuickTools session.
5. Open an Internet browser again and log in with the new IP address.

CLI Switch Configuration

To configure the switch using the command line interface, do the following:

1. Open a command window according to the type of workstation and connection:
   - Ethernet (all platforms): Open a Telnet session with the default switch IP address and log in to the switch with default account name and password (admin/password).

     ```
     telnet 10.0.0.1
     Switch Login: admin
     Password:     *******
     ```

     NOTE:

     To insure fabric security, you should change the password for the Admin account name. Refer to the Passwd command in the *SANbox 5802V Fibre Channel Switch Command Line Interface Guide*

   - Serial – Windows: Open the HyperTerminal application on a Windows platform.
     a. Choose the **Start** button, select **Programs, Accessories, HyperTerminal,** and **HyperTerminal**.
     b. Select the connection you created earlier and choose the **OK** button.

- Serial – Linux: Open a command window and enter the following command:

```
minicom
```

- Serial – Solaris: Open a command window and enter the following command:

```
tip hardwire
```

2. Open an admin session and enter the Set Setup System command. Enter the values you want for switch IP address (EthNetworkAddress) and the network mask (EthNetworkMask). Refer to the *SANbox 5802V Fibre Channel Switch Command Line Interface Guide* for more information about the CLI commands.

```
SANbox #> admin start
SANbox (admin) #> set setup system
```

3. Open a Config Edit session and use the Set Config Switch command to modify the switch configuration.

Cable Devices to the Switch

Connect cables to the SFP transceivers and their corresponding devices, and then energize the devices. Device host bus adapters can have SFP (or SFF) transceivers. LC-type duplex fiber optic cable connectors are designed for SFP transceivers. Duplex cable connectors are keyed to ensure proper orientation. Choose the fiber optic cable with the connector combination that matches the device host bus adapter.

GL_Ports self configure as FL_Ports when connected to loop of devices or F_Ports when connected to a single device. G_Ports self configure as F_Ports when connected to a single device. Both GL_Ports and G_Ports self configure as E_Ports when connected to another switch.

Installing Firmware

The switch comes with current firmware installed. You can upgrade the firmware from the management workstation as new firmware becomes available. You can use the CLI or QuickTools to install new firmware.

- Using QuickTools to Install Firmware
- Using the CLI to Install Firmware

You can load and activate firmware upgrades on an operating switch without disrupting data traffic or re-initializing attached devices. If you attempt to perform a non-disruptive activation without satisfying the following conditions, the activation will fail. If the non-disruptive activation fails, you will usually be prompted to try again later. Otherwise, the switch will perform a disruptive activation.

- The current firmware version permits the installation and non-disruptive activation of the new firmware. Refer to the *Firmware Release Notes* for previous compatible firmware versions.
- No changes are being made to switches in the fabric including powering up, powering down, disconnecting or connecting ISLs, changing switch configurations, or installing firmware.
- No port in the fabric is in the diagnostic state.
- No Zoning Edit sessions are open in the fabric.
- No changes are being made to attached devices including powering up, powering down, disconnecting, connecting, and HBA configuration changes.

Install firmware on one switch at a time in the fabric. If you are installing firmware on one switch, wait 120 seconds after the activation is complete before installing firmware on a second switch.

Ports that are stable when the non-disruptive activation begins and then change states, will be reset. When the non-disruptive activation is complete, Enterprise Fabric Suite 2007 and QuickTools sessions reconnect automatically. However, Telnet sessions must be restarted manually.

NOTE:

After upgrading firmware that includes changes to QuickTools, an open QuickTools session may indicate that the firmware is not supported. This means the new firmware is not supported by the previous QuickTools version. To correct this, close the QuickTools session and the browser window, then open a new QuickTools session.

Using QuickTools to Install Firmware

To install firmware using QuickTools, do the following:

1. In the faceplate display, open the Switch menu and select **Load Firmware**.
2. In the Firmware Upload dialog, click the **Browse** button to browse and select the firmware file to be uploaded.
3. Click the **Start** button to begin the firmware load process. You will be shown a message warning you that the switch will be reset to activate the firmware.
4. QuickTools prompts you to activate the new firmware using a hot (non-disruptive) reset, if possible. Click the **OK** button to reset the switch and activate the new firmware.

Using the CLI to Install Firmware

The method you choose to install firmware using the CLI depends on the type of firmware activation you want.

- For a disruptive activation, enter the Firmware Install or Image Install command to download the firmware image file from an FTP or TFTP server, unpack it, and activate it in one step. Refer to “One-Step Firmware Installation” on page 4-16.
- For a non-disruptive activation, enter the Image Fetch command to download the firmware image file from an FTP or TFTP server. Enter the Image Unpack command to unpack the image file, then enter the Hotreset command to perform a non-disruptive activation. Refer to “Custom Firmware Installation” on page 4-18.

Refer to the *SANbox 5802V Fibre Channel Switch Command Line Interface Guide* for information about the CLI commands.

One-Step Firmware Installation

The Firmware Install and Image Install commands download the firmware image file from an FTP or TFTP server to the switch, unpacks the image file, and performs a disruptive activation in one step. The installation process prompts you to enter the following:

- The file transfer protocol (FTP or TFTP)
- IP address of the remote host
- An account name and password on the remote host (FTP only)
- Pathname for the firmware image file

To install firmware using the CLI when a File Transfer Protocol (FTP) server is present on the management workstation, use the Firmware Install command. Refer to the *SANbox 5802V Fibre Channel Switch Command Line Interface Guide* for information about the CLI commands.

1. Enter the following commands to download the firmware from a remote host to the switch, install the firmware, then reset the switch to activate the firmware.

```
SANbox #> admin start
SANbox #> firmware install
  The switch will be reset. This process will cause a
  disruption to I/O traffic.
  Continuing with this action will terminate all management
  sessions,including any Telnet sessions. When the firmware
  activation is complete, you may log in to the switch again.
  Do you want to continue? [y/n]: y
  Press 'q' and the ENTER key to abort this command.
```

2. Enter your choice for the file transfer protocol with which to download the firmware image file. FTP requires an user account and a password; TFTP does not.

```
  FTP or TFTP     : ftp
```

3. Enter your account name on the remote host (FTP only) and the IP address of the remote host. When prompted for the source file name, enter the path for the firmware image file.

```
  User Account    : johndoe
  IP Address      : 10.0.0.254
  Source Filename : 7.2.00.11_epc
  About to install image.  Do you want to continue? [y/n] y
```

4. When prompted to install the new firmware, enter Yes to continue or No to cancel. Entering Yes will disrupt traffic. This is the last opportunity to cancel.

```
About to install image. Do you want to continue? [y/n] y
Connected to 10.20.20.200 (10.20.20.200).
220 localhost.localdomain FTP server (Version wu-2.6.1-18)
ready.
```

5. Enter the password for your account name (FTP only).

```
331 Password required for johndoe.
Password:******
230 User johndoe logged in.
```

6. The firmware will now be downloaded from the remote host to the switch, installed, and activated.

Custom Firmware Installation

A custom firmware installation downloads the firmware image file from an FTP or TFTP server to the switch, unpacks the image file, and resets the switch in separate steps. This allows you to choose the type of switch reset and whether the activation will be disruptive (Reset Switch command) or non-disruptive (Hotreset command). The following example illustrates a custom firmware installation with a non-disruptive activation.

1. Download the firmware image file from the workstation to the switch.

   - If your workstation has an FTP server, you can enter the Image Fetch command:

     `SANbox (admin) #> **image fetch account_name ip_address filename**`

   - If your workstation has a TFTP server, you can enter the Image TFTP command to download the firmware image file.

     `SANbox (admin) #> **image tftp ip_address filename**`

   - If your workstation has neither an FTP nor a TFTP server, open an FTP session and enter FTP commands:

     `>ftp ***ip_address*** or ***switchname***`
     `user:**images**`
     `password: **images**`
     `ftp>**bin**`
     `ftp>**put *filename***`
     `ftp>**quit**`

2. Display the list of firmware image files on the switch to confirm that the file was loaded.

   `SANbox (admin) $>**image list**`

3. Unpack the firmware image file to install the new firmware in flash memory.

   `SANbox (admin) $>**image unpack *filename***`

4. Wait for the unpack to complete.

   `image unpack command result: Passed`

5. A message will prompt you to reset the switch to activate the firmware. Use the Hotreset command to attempt a non-disruptive activation.

   `SANbox (admin) $>**hotreset**`

Adding a Switch to an Existing Fabric

If there are no special conditions to be configured for the new switch, simply plug in the switch and the switch becomes functional with the default fabric configuration. The default fabric configuration settings are as follows:

- Fabric zoning is sent to the switch from the fabric
- All ports will be GL_Ports
- The default IP address 10.0.0.1 is assigned to the switch without a gateway or boot protocol configured (RARP, BOOTP, and DHCP).

If you are adding a switch to a fabric and do not want to accept the default fabric configuration, do the following:

1. If the switch is not new from the factory, reset the switch to the factory configuration before adding the switch to the fabric.
2. If you want to manage the switch through the Ethernet port, you must first configure the IP address.
3. Plug in the inter-switch links (ISL), but do not connect the devices.
4. Configure the port types for the new switch. The ports can be G_Port, GL_Port, F_Port, FL_Port, or Donor.
5. Connect the devices to the switch.
6. Make any necessary zoning changes.

Installing Feature License Keys

Refer to “Feature Licensing” on page 3-5 for information about available license keys. To install a license key using QuickTools, do the following:

1. Open the Switch Menu and select **Features** to open the Feature Licenses dialog.
2. In the Feature Licenses dialog, click the **Add** button to open the Add License Key dialog.
3. In the Add License Key dialog, enter the license key in the Key field.
4. Click the **Get Description** button to display the upgrade description.
5. Click the **Add** button to upgrade the switch. Allow a minute or two for the upgrade to complete.

To upgrade a switch using the command line interface, refer to the Feature command in the *SANbox 5802V Fibre Channel Switch Command Line Interface Guide*.

Notes

5 Diagnostics/Troubleshooting

Diagnostic information about the switch is available through the chassis LEDs and the port LEDs. Diagnostic information is also available through the CLI, or QuickTools event logs and error displays. This section describes the following types of diagnostics:

- Chassis Diagnostics describes the Input Power LED and System Fault LED indications.
- Power-On Self Test Diagnostics describe the Heartbeat LED and the port Logged-In LED indications.
- Power Supply Diagnostics describes Power Supply Status LED and Power Supply Fault LED indications.

This section also describes using maintenance mode to recover a disabled switch.

Chassis Diagnostics

Chassis diagnostics are indicated by the chassis LEDs as shown in Figure 5-1.

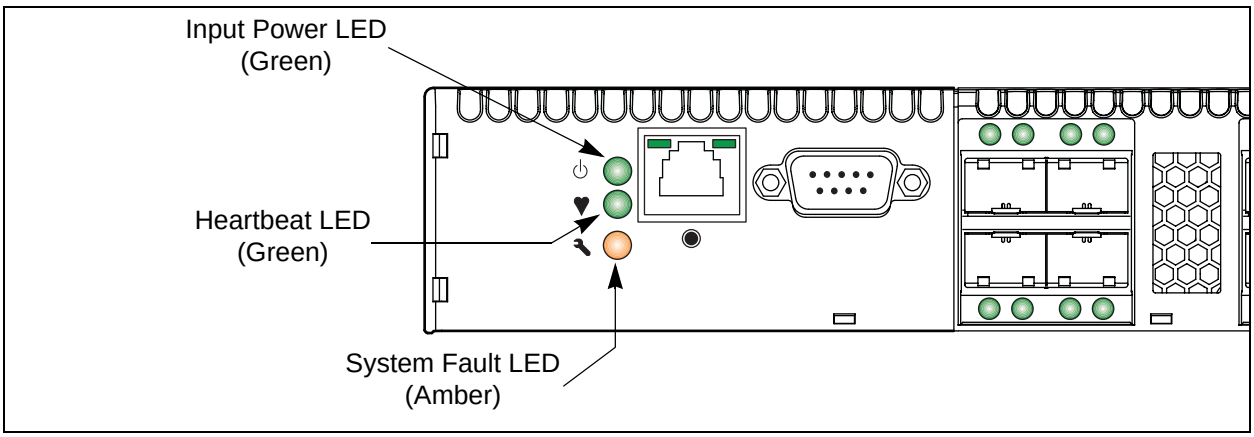


Figure 5-1 Chassis LEDs

The following conditions are described:

- Input Power LED Is Extinguished
- System Fault LED Is Illuminated

Input Power LED Is Extinguished

The Input Power LED illuminates to indicate that the switch logic circuitry is receiving proper voltages. If the Input Power LED is extinguished, do the following:

1. Inspect the power cords and connectors. Is the cord unplugged? Is the cord or connector damaged?
   - Yes - Make necessary corrections or repairs. If the condition remains, continue.
   - No - Continue.
2. Inspect the AC power source. Is the power source delivering the proper voltage?
   - Yes - Continue.
   - No - Make necessary repairs. If the condition remains, continue.
3. Inspect the power supplies. Are the power supplies fully seated in their bays?
   - Yes - Continue. Replace the power supplies.
   - No - Reinstall the power supplies. If the condition remains, replace the power supplies.

System Fault LED Is Illuminated

The System Fault LED illuminates to indicate that a fault exists in the switch firmware or hardware. If the System Fault LED illuminates, do the following:

- Check the Heartbeat LED for an error blink pattern and take the necessary actions. Refer to “Heartbeat LED Blink Patterns” on page 5-3.
- Check the power supply LEDs and take the necessary actions. Refer to “Power Supply Diagnostics” on page 5-12.

Power-On Self Test Diagnostics

The switch performs a series of tests as part of its power-up procedure. The POST diagnostic program performs the following tests:

- Checksum tests on the boot firmware in Programmable Read Only Memory (PROM) and the switch firmware in flash memory
- Internal data loopback test on all ports
- Access and integrity test on the Application Specific Integrated Circuit (ASIC)

During the POST, the switch logs any errors encountered. Some POST errors are critical, others are not. The switch uses the Heartbeat LED and the Logged-In LED to indicate switch and port status. A critical error disables the switch so that it will not operate. A non-critical error allows the switch to operate, but disables the ports that have errors. If two or more ports fail the POST, the entire switch is disabled. Whether the problem is critical or not, contact your authorized maintenance provider.

If there are no errors, the Heartbeat LED blinks at a steady rate of once per second. If a critical error occurs, the Heartbeat LED will show a blink pattern that indicates an error and the System Fault LED will illuminate. If there are non-critical errors, the switch disables the failed ports and flashes the associated Logged-In LEDs. Refer to “Heartbeat LED Blink Patterns” on page 5-3 for more information about Heartbeat LED blink patterns.

Heartbeat LED Blink Patterns

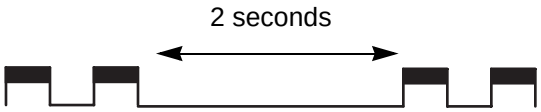
The Heartbeat LED indicates the operational status of the switch. When the POST completes with no errors, the Heartbeat LED blinks at steady rate of once per second. When the switch is in maintenance mode, the Heartbeat LED illuminates continuously. Refer to “Recovering a Switch Using Maintenance Mode” on page 5-13 for more information about maintenance mode. All other blink patterns indicate critical errors. In addition to producing a heartbeat error blink patterns, a critical error also illuminates the System Fault LED.

The Heartbeat LED shows an error blink pattern for the following conditions:

- 1 blink – Normal operation
- 2 blinks – Internal Firmware Failure Blink Pattern
- 3 blinks – Fatal POST Error Blink Pattern
- 4 blinks – Configuration File System Error Blink Pattern
- 5 blinks – Over Temperature Blink Pattern

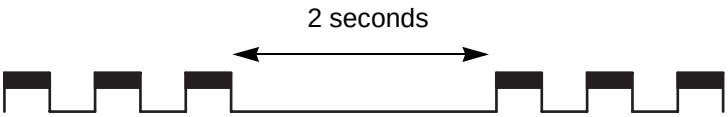
Internal Firmware Failure Blink Pattern

An internal firmware failure blink pattern is 2 blinks followed by a two second pause. The 2-blink error pattern indicates that the firmware has failed, and that the switch must be reset. Momentarily press and release the Maintenance button to reset the switch.



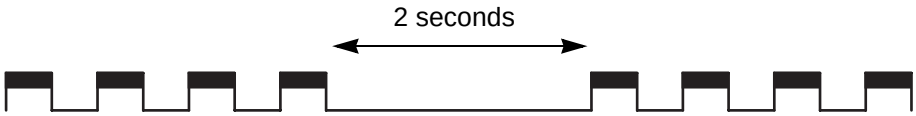
Fatal POST Error Blink Pattern

A system error blink pattern is 3 blinks followed by a two second pause. The 3-blink error pattern indicates that a POST failure or a system error has left the switch inoperable. If a system error occurs, contact your authorized maintenance provider. Momentarily press and release the Maintenance button to reset the switch.



Configuration File System Error Blink Pattern

A configuration file system error blink pattern is 4 blinks followed by a two second pause. The 4-blink error pattern indicates that a configuration file system error has occurred, and that the configuration file must be restored.



To restore the switch configuration, do the following:

1. Establish communications with the switch using Telnet. Enter one of the following on the command line:

   `telnet` *`xxx.xxx.xxx.xxx`*
   or

   `telnet` *`switchname`*

   where *xxx.xxx.xxx.xxx* is the switch IP address and *switchname* is the switch name associated with the IP address.

2. A Telnet window opens prompting you for a login. Enter an account name and password. The default account name and password are *admin* and *password*.

3. Open an admin session to acquire the necessary authority.

   ```
   SANbox $>admin start
   ```

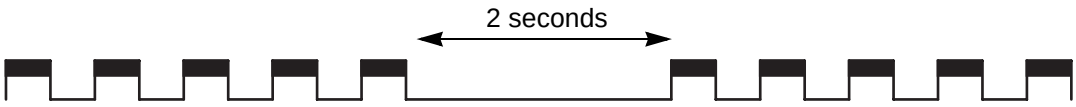
4. Restore the configuration. When the restore is complete, the switch will reset.

   ```
   SANbox (admin) $>config restore
   ```

   If a configuration does not exist, enter the Config Backup command, then enter the Config Restore command.

Over Temperature Blink Pattern

An over temperature blink pattern is 5 blinks followed by a two second pause. The 5-blink error pattern indicates that the air temperature inside the switch has exceeded the failure temperature threshold.



If the Heartbeat LED shows the over temperature blink pattern, do the following:

1. Inspect the chassis vents. Are the intake and exhaust vents clear?
   - Yes - Continue.
   - No - Remove any debris from fan intake and exhaust if necessary. If the condition remains, continue.
2. Inspect the Power Supply Fault LED on both power supplies. Is the Power Supply Fault LED illuminated on either power supply?
   - Yes - Replace the power supply. If the condition remains, continue.
   - No - Continue.
3. Observe the air flow direction from both power supplies. Are they the same?
   - Yes - Continue.
   - No - Determine the proper air flow direction for the switch. Replace the power supply with the incorrect air flow direction with another having the correct air flow direction. Air flow direction is marked on the power supply part number label. If the condition remains, continue.
4. Consider the ambient air temperature near the switch and clearance around the switch. Make necessary corrections. If the condition remains, open a command line window and log on to the switch. Enter the Shutdown command, then power down the switch. Contact your authorized maintenance provider.

Logged-In LED Indications

Port diagnostics are indicated by the Logged-In LED for SFP and XPAK ports as shown in Figure 5-2.

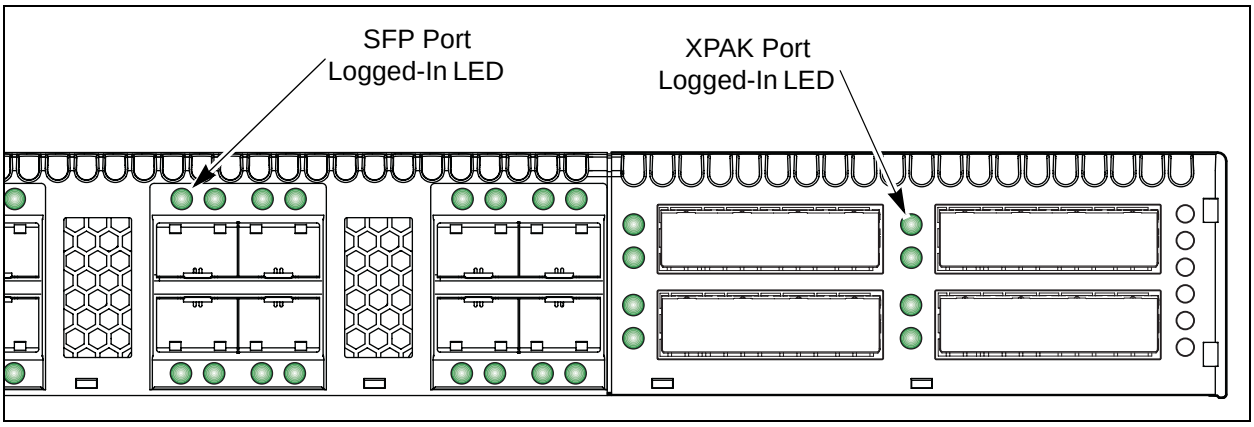


Figure 5-2 Logged-In LED

The Logged-In LED has three indications:

- Continuous illumination: A device is logged in to the port.
- Flashing once per second: A device is logging in to the port, or the port is in the diagnostics state.
- Flashing twice per second: The port is down, offline, or an error has occurred.

If a Logged-In LED is flashing twice per second, review the event browser for alarm messages regarding the affected port. You can also inspect the alarm log using the Show Alarm command. If there is an error, alarm messages may point to one or more of the following conditions:

- E_Port Isolation
- Excessive Port Errors

E_Port Isolation

A Logged-In LED error indication is often the result of E_Port isolation. E_Port isolation can be caused by the following:

- Security failure
- A port configured as FL_Port is connected to another switch
- Conflicting domain IDs
- Conflicting timeout values
- Conflicting zone membership between active zone sets

Using QuickTools, review the event browser, and do the following to diagnose and correct an isolated E_Port:

1. Does the event browser show an alarm about an invalid attach on the affected port?
   - Yes - If device security is configured, review the ISL group in the active security set to ensure that the membership includes the necessary ports and that the secrets on all switches are correct.
   - No - Continue.
2. Does the event browser show a repeating alarm about an unsupported E_Port command on the affected port?
   - Yes - The port is configured as an FL_Port and connected to another switch. Correct the port connection or the port type.
   - No - Continue.
3. Display the fabric domain IDs using the Show Domains command, or click the **Switch** tab and Summary icon in QuickTools. Are all domain IDs in the fabric unique?
   - Yes - Continue.
   - No - Correct the domain IDs on the offending switches using the Set Config Switch command. Reset the port. If the condition remains, continue.
4. Compare the RA_TOV and ED_TOV timeout values for all switches in the fabric using the Show Config Switch command, or click the **Switch** tab and Advanced icon in QuickTools. Is each timeout value the same on every switch?
   - Yes - Continue.
   - No - Correct the timeout values on the offending switches using the Set Config Switch CLI. Reset the port. If the condition remains, continue.

5. Display the active zone set on each switch using the Zoning Active command, or click the **Active Zoneset** tab in QuickTools. Compare the zone membership between the two active zone sets. Are they the same?
   - Yes - Contact your authorized maintenance provider.
   - No - Deactivate one of the active zone sets or edit the conflicting zones so that their membership is the same, then reset the port. If the condition remains, contact your authorized maintenance provider.

NOTE:

E_Port isolation can be caused by merging two fabrics whose active zone sets have two zones with the same name, but different membership.

Excessive Port Errors

The switch can monitor a set of port errors and generate alarms based on user-defined sample windows and thresholds. These port errors include the following:

- Cyclic Redundancy Check (CRC) errors
- Decode errors
- ISL connection count
- Device login errors
- Device logout errors
- Loss-of-signal errors

Port threshold alarm monitoring is disabled by default. Refer to the *SANbox 5802V Fibre Channel Switch Command Line Interface Guide* for information about managing port threshold alarms.

If the count for any of these errors exceeds the rising trigger for three consecutive sample windows, the switch generates an alarm and disables the affected port, changing its operational state to *down*. Port errors can be caused by the following:

- Triggers are too low or the sample window is too small
- Faulty Fibre Channel port cable
- Faulty SFP
- Faulty port
- Faulty device or HBA

Review the event browser to determine if excessive port errors are responsible for disabling the port. Look for a message that mentions one of the monitored error types indicating that the port has been disabled, then do the following:

1. Examine the alarm configuration for the associated error using the Show Config Threshold command. Refer to the Show Config Threshold command in the *SANbox 5802V Fibre Channel Switch Command Line Interface Guide*. Are the thresholds and sample window correct?
   - Yes - Continue
   - No - Correct the alarm configuration. If the condition remains, continue.
2. Reset the port, then perform an external port loopback test to validate the port and the SFP. Refer to the *SANbox 5802V Fibre Channel Switch Command Line Interface Guide* or the *SANbox 5802V QuickTools Switch Management User Guide* for information about testing ports. Does the port pass the test?
   - Yes - Continue
   - No - Replace the SFP and repeat the test. If the port does not pass the test, contact your authorized maintenance provider. Otherwise continue.
3. Replace the Fibre Channel port cable. Is the problem corrected?
   - Yes - Complete.
   - No - Continue.
4. Inspect the device to which the affected port is connected and confirm that the device and its HBA are working properly. Make repairs and corrections as needed. If the condition remains, contact your authorized maintenance provider.

Transceiver Diagnostics

NOTE:

Transceiver diagnostic information is available with purchase of the SANdoctor license key. To purchase a license key, contact your authorized maintenance provider.

You can display the following transceiver information using the Show Media CLI command:

- Port number
- Manufacturer
- Temperature (°C)
- Operating voltage (volts)
- Transmitter bias (milliamps)
- Transmitter power (milliwatts)
- Receiver power (milliwatts)

The display indicates warning and alarm conditions for both high and low values.

Power Supply Diagnostics

A power supply has a Status LED (Green) and a Fault LED (Amber) as shown in Figure 5-3. Under normal operating conditions, the Power Supply Status LED is illuminated and the Power Supply Fault LED is extinguished.

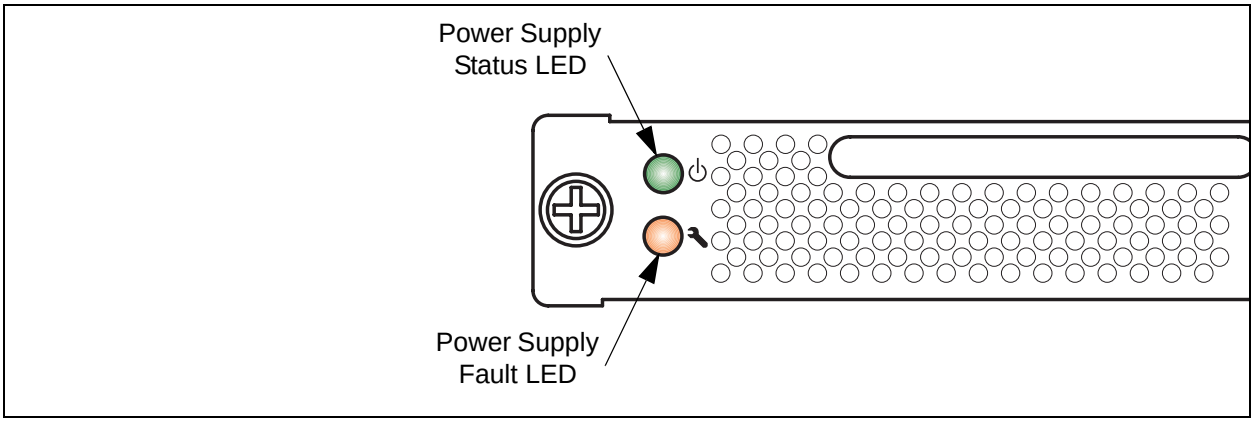


Figure 5-3 Power Supply LEDs

Consider the following indications:

- All power supply LEDs are normal, yet the System Fault LED is illuminated and the Heartbeat LED does not show a blink pattern. This means that the two power supplies have different air flow directions. Replace the power supply with the incorrect air flow direction with another having the correct air flow direction. Air flow direction is marked on the power supply part number label. Refer to “Power Supply Removal and Replacement” on page 6-2.
- Power Supply Fault LED is illuminated. This means that the power supply is failing or has failed. Replace the power supply with another having the same air flow direction. Air flow direction is indicated on the power supply part number label. Refer to “Power Supply Removal and Replacement” on page 6-2.

Recovering a Switch Using Maintenance Mode

A switch can become inoperable or unmanageable for the following reasons:

- Firmware becomes corrupt
- IP address is lost
- Switch configuration becomes corrupt
- Password forgotten

In these specific cases, you can recover the switch using maintenance mode. Maintenance mode temporarily returns the switch IP address to 10.0.0.1 and provides opportunities to do the following:

- Exiting the Maintenance Menu (Option 0)
- Unpacking a Firmware Image File in Maintenance Mode (Option 1)
- Resetting the Network Configuration in Maintenance Mode (Option 2)
- Resetting User Accounts in Maintenance Mode (Option 3)
- Copying Log Files in Maintenance Mode (Option 4)
- Removing the Switch Configuration in Maintenance Mode (Option 5)
- Remaking the File System in Maintenance Mode (Option 6)
- Resetting the Switch in Maintenance Mode (Option 7)
- Updating the Boot Loader in Maintenance Mode (Option 8)

To recover a switch, do the following:

1. Place the switch in maintenance mode. Press and hold the Maintenance button with a pointed tool until only the Heartbeat LED is illuminated, and then release the button. The Heartbeat LED illuminates continuously when the switch is in maintenance mode.
2. Establish a Telnet session with the switch using the maintenance mode IP address 10.0.0.1.
3. Enter the maintenance mode account name and password (*prom*, *prom*), and press the Enter key.

```
Switch login: prom
Password:xxxx
```

4. The maintenance menu displays several recovery options. To select a switch recovery option, press the corresponding number (displayed in option: field) on the keyboard and press the Enter key.

```
0)  Exit
1)  Image Unpack
2)  Reset Network Config
3)  Reset User Accounts to Default
4)  Copy Log Files
5)  Remove Switch Config
6)  Remake Filesystem
7)  Reset Switch
8)  Update Boot Loader
Option:
```

These options and their use are described in the following subsections.

Exiting the Maintenance Menu (Option 0)

The Exit option closes the current Maintenance menu session. To log in again, enter the maintenance mode account name and password (prom, prom). To return to normal operation, momentarily press and release the Maintenance button or power cycle the switch.

Unpacking a Firmware Image File in Maintenance Mode (Option 1)

The Image Unpack option unpacks and installs new firmware when the current firmware has become corrupt. Before using this option, you must load the new firmware image file onto the switch. The steps to install new firmware using this option are as follows:

1. Place the switch in maintenance mode. Refer to the procedure for maintenance mode in “Recovering a Switch Using Maintenance Mode” on page 5-13.
2. Use FTP to load a new firmware image file onto the switch. Refer to “Custom Firmware Installation” on page 4-18 for an example of how to load the image file. When the download is complete, close the FTP session.
3. Establish a Telnet session with the switch using the default IP address 10.0.0.1.

```
telnet 10.0.0.1
```

4. Enter the maintenance mode account name and password (*prom*, *prom*), and press the Enter key.

```
Switch login: prom
Password:xxxx
```

5. Select option 1 from the maintenance menu. When prompted for a file name prompt, enter the firmware image file name.

```
Image filename: filename
Unpacking 'filename', please wait...
Unpackage successful.
```

6. Select option 7 to reset the switch and exit maintenance mode.

Resetting the Network Configuration in Maintenance Mode (Option 2)

The Reset Network Config option resets the network properties to the factory default values and saves them on the switch. Refer to *SANbox 5802V Fibre Channel Switch Command Line Interface Guide* for the default network configuration values.

Resetting User Accounts in Maintenance Mode (Option 3)

The Reset User Accounts to Default option restores the password for the Admin account name to the default (password) and removes all other user accounts from the switch.

Copying Log Files in Maintenance Mode (Option 4)

The Copy Log Files option copies all log file buffers to a file on the switch named *logfile*. You can use FTP to download this file to the management workstation, however, you must download the logfile before resetting the switch. Refer to the *SANbox 5802V Fibre Channel Switch Command Line Interface Guide* for information about downloading files from the switch.

Removing the Switch Configuration in Maintenance Mode (Option 5)

The Remove Switch Config option deletes all configurations from the switch except the default configuration. This restores switch configuration parameters to the factory defaults. Refer to Reset command in the *SANbox 5802V Fibre Channel Switch Command Line Interface Guide* for the factory default values.

Remaking the File System in Maintenance Mode (Option 6)

In the event of a loss of power, the switch configuration may become corrupt. The file system on which the configuration is stored must be re-created. The Remake Filesystem option resets the switch to the factory default values, including user accounts and zoning. Refer to the Reset command in the *SANbox 5802V Fibre Channel Switch Command Line Interface Guide* for the factory default values.

CAUTION!

If you choose the **Remake Filesystem** option, you will lose all changes made to the fabric configuration that involve that switch, such as password and zoning changes. You must then restore the switch from an archived configuration or reconfigure the portions of the fabric that involve the switch.

Resetting the Switch in Maintenance Mode (Option 7)

The Reset Switch option closes the Telnet session, exits maintenance mode, and reboots the switch using the current switch configuration. All unpacked firmware image files that reside on the switch are deleted.

Updating the Boot Loader in Maintenance Mode (Option 8)

The Update Boot Loader option updates the system boot loader which loads the Linux kernel into memory. Use this option only at the direction of your authorized maintenance provider.

6 Removal/Replacement

This section describes the removal and replacement procedures for the following field replaceable units (FRU):

- SFP and XPAK transceivers
- Power supplies

The switch is equipped with a battery that powers the non-volatile memory. This memory stores the switch configuration. The battery is not a field replaceable unit.

WARNING!!

Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of the used battery according to the manufacturer's instructions.

WARNUNG!!

Bei unsachgemäß ausgetauschter Batterie besteht Explosionsgefahr. Die Batterie nur mit der gleichen Batterie oder mit einem äquivalenten, vom Hersteller empfohlenen Batterietyp ersetzen. Die gebrauchte Batterie gemäß den Herstelleranweisungen entsorgen.

AVERTISSEMENT!!

Danger d'explosion si le remplacement de la pile est incorrect. Ne remplacer que par une pile de type identique ou équivalent recommandé par le fabricant. Jeter la pile usagée en observant les instructions du fabricant.

¡ADVERTENCIA!

Peligro de la explosión si la batería es reemplazada incorrectamente. Substituya solamente con el mismo tipo o equivalente recomendado por el fabricante. Deshágase de la batería usada según las instrucciones del fabricante.

Transceiver Removal and Replacement

The SFP and XPAK transceivers can be removed and replaced while the switch is operating without damaging the switch or the transceiver. However, transmission on the affected port will be interrupted until the transceiver installed.

To remove a transceiver, gently press the transceiver into the port to release the tension, then pull on the release tab or lever and remove the transceiver. Different transceiver manufacturers have different release mechanisms. Consult the documentation for your transceiver. To install, insert the transceiver into the port and gently press until it snaps in place.

NOTE:

The SFP and XPAK transceivers will fit only one way. If the transceiver does not install under gentle pressure, flip it over and try again.

Power Supply Removal and Replacement

The power supplies are hot pluggable. This means you can remove or install one of the power supplies while the switch is operating without disrupting service. The power supplies are also interchangeable; that is, the left and right power supplies are the same unit.

CAUTION!

- Both power supplies must have the same air flow direction to prevent the switch from overheating.
- To avoid overheating, do not operate the switch with one power supply any longer than necessary.

When removing or replacing a power supply, consider the following:

- The left and right power supplies are interchangeable. However, you must orient the power supply so that AC receptacle is on the right.
- Both power supplies must have the same air flow direction. The part number label on the power supply indicates the air flow direction.
- When removing or replacing a power supply on an operating switch, be sure the Heartbeat LED is showing the normal 1 blink per second. This allows the switch to correctly report power supply status.

To remove a power supply, unplug the power supply and loosen the two knurled fasteners with a cross-head screw driver as shown in Figure 6-1. Grasp the power supply handle and pull firmly to disengage the modular connector. Slide the power supply out of its bay.

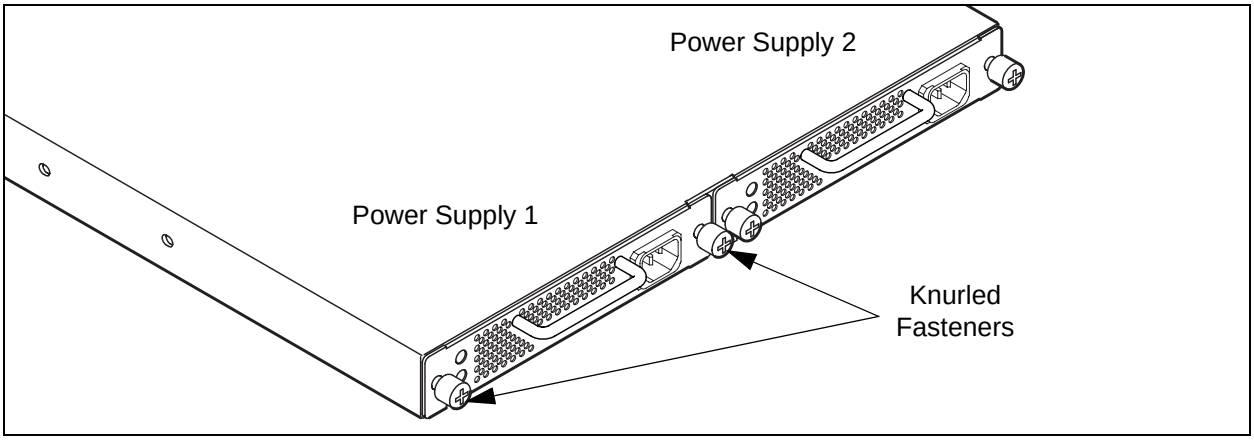


Figure 6-1 Power Supply Removal

1. Confirm that the Heartbeat LED is showing the normal 1 blink per second. This allows the switch to correctly report power supply status.
2. Confirm that the new power supply is compatible with the switch air flow direction. The part number label on the power supply indicates the air flow direction as shown in Figure 6-2.
3. With the AC receptacle on the right, slide the power supply into the bay until it is firmly seated. Secure the knurled fasteners by hand.
4. Plug the power cord into the AC receptacle. Confirm that air flow is correct.

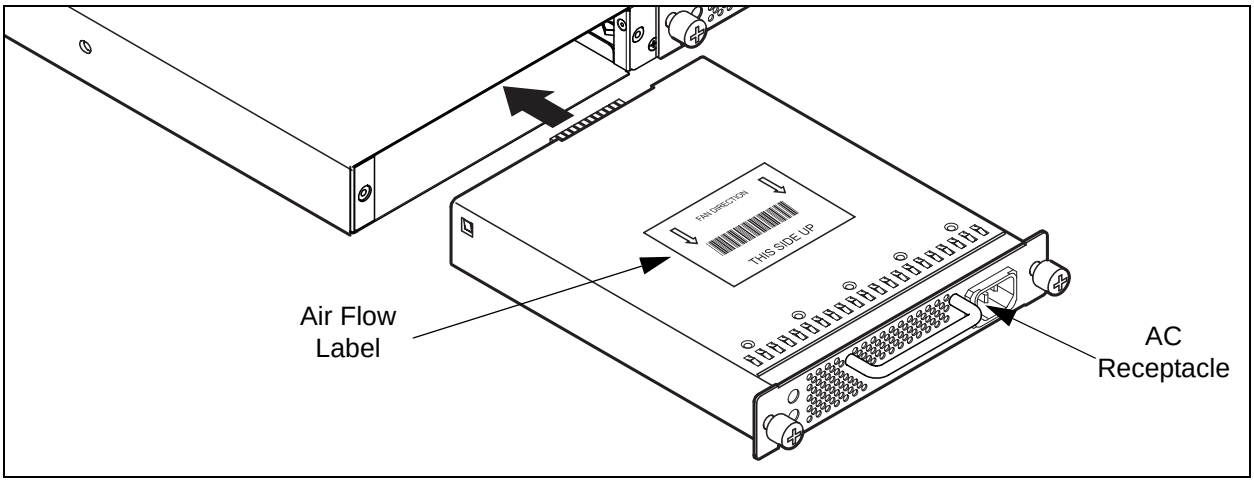


Figure 6-2 Power Supply Installation

Notes

A Specifications

This appendix contains the specifications for the SANbox 5802V Fibre Channel switch. Refer to Section 2 for the location of all connections, switches, controls, and components.

- Fabric Specifications
- Maintainability
- Fabric Management
- Dimensions
- Electrical
- Power Cord Specifications
- Environmental
- Regulatory Certifications

Fabric Specifications

Table A-1. Fabric Specifications

Fibre Channel Protocols	FC-AL Rev 4.6 FC-AL-2 Rev 7.0 FC-DA FC-FLA FC-FS-2 FC-GS-5 FC-FG FC-LS FC-MI-2 FC-PH Rev. 4.3 FC-PH-2 FC-PH-3 FC-PI-3 FC-SP FC-Tape FC-VI FC-SW-4 Fibre Channel Element MIB RFC 2837 Fibre Alliance MIB Version 4.0
Fibre Channel Classes of Service	Classes 2 and 3
Modes of Operation	Fibre Channel Classes 2 and 3, connectionless
Port Types	
■ SFP Ports	G_Port, GL_Port, F_Port, FL_Port, E_Port
■ XPAK Ports	G_Port, F_Port, E_Port
Port Characteristics	All ports are auto-discovering and self-configuring.
Number of Fibre Channel Ports	■ Twenty 2/4/8-Gbps SFP ports ■ Four 10-Gbps XPAK ports (upgradable to 20-Gbps)

Table A-1. Fabric Specifications (Continued)

Scalability	Maximum 239 switches depending on configuration
Maximum User Ports	> 475,000 ports depending on configuration
Buffer Credits	16 buffer credits per port, ASIC embedded memory
Media Type	
Ports 0-19	SFP optical transceiver
Ports 20-23	XPAK switch stacking cables
Fabric Port Speed	
Ports 0-19	2.125, 4.250, or 8.50 Gbps
Ports 20-23	12.750 or 25.50 Gbps
Maximum Frame Size	2148 bytes (2112 byte payload)
System Processor	400 MHz 440EP processor
Fabric Latency (intra-switch)	
2-Gbps to 2-Gbps	< 0.6 µsec
4-Gbps to 4-Gbps	< 0.3 µsec
8-Gbps to 8-Gbps	< 0.2 µsec
10-Gbps to 10-Gbps	< 0.2 µsec
20-Gbps to 20-Gbps	< 0.2 µsec
Bandwidth	
Point-to-Point	425 MB, Full Duplex @ 2-Gbps 850 MB, Full Duplex @ 4-Gbps 1700 MB, Full Duplex @ 8-Gbps 2550 MB, Full Duplex @ 10-Gbps 5100 MB, Full Duplex @ 20-Gbps
Aggregate (single switch)	Up to 23.80 GB Full Duplex

Maintainability

Table A-2. Maintainability Specifications

Diagnostics	Power-On Self Test (POST) tests all functional components except SFP transceivers. Port tests include online, internal, and external tests.
User Interface	LED indicators
Field Replaceable Units	Power supplies

Fabric Management

Table A-3. Fabric Management Specifications

Management Methods	QuickTools web applet Command Line Interface Application Programming Interface SMI-S GS-3 Management Server SNMP FTP TFTP
Maintenance Connection	RS-232 connector; null modem F/F DB9 cable
Ethernet Connection	RJ-45 connector; 10/100 BASE-T cable
Switch Agent	Allows a network management station to obtain configuration values, traffic information, and failure data pertaining to the Fibre Channels using SNMP through the Ethernet interface.

Dimensions

Table A-4. Dimensional Specifications

Width.....	17” (432 mm), 19 inch rack mount
Height	1.70” (43.2 mm) (1U)
Depth	19.69” (500 mm)
Weight.....	18 lbs (8.16 Kg)

Electrical

Table A-5. Electrical Specifications

Operating voltage	100 to 240 VAC; 50 to 60 Hz
Power source loading (maximum) ..	1 A at 120 VAC 0.5 A at 240 VAC
Heat Output (maximum)	120 watts
Circuit Protection	Internally fused

Power Cord Specifications

The switch comes with one or two power cords with NEMA 5-15 non-locking plugs (SKU: CPK-9000-US). This power cord is approved for North America (USA, Canada, Puerto Rico), Mexico, Central America, South America, Korea, Taiwan, Phillippines, and Thailand. A similar power cord with a locking plug is also available ((SKU: CPK-9000-USL). QLogic offers power cords for additional regions/countries as listed in Table A-6.

Table A-6. Availalbe Power Cords

Region/Country	Specification	QLogic SKU Number
Argentina	IRAM 2073.1982 Plug	CPK-9000-AR
Australia	AS/NZS 3112 Plug	CPK-9000-AUNZ
Bahrain	BS1363/A Plug	CPK-9000-UKHK
China (PRC)	GB2099/GB1002-1 Plug	CPK-9000-CN
Denmark	Data DK-2-5A Plug	CPK-9000-DK

Table A-6. Availalbe Power Cords (Continued)

Region/Country	Specification	QLogic SKU Number
Europe	CEE 7/7 Plug	CPK-9000-CEE
Finland	CEE 7/7 Plug	CPK-9000-CEE
Greece	CEE 7/7 Plug	CPK-9000-CEE
Hong Kong/Macau (PRC)	BS1363/A Plug	CPK-9000-UKHK
Hungary	BS1363/A Plug	CPK-9000-UKHK
India	BS 546 Plug	CPK-9000-ZAIN
Indonesia	CEE 7/7 Plug	CPK-9000-CEE
International (special)	IEC 60309 Plug	CPK-9000-IEC
Ireland (Northern)	AS/NZS 3112 Plug	CPK-9000-AUNZ
Ireland (Southern)	BS1363/A Plug	CPK-9000-UKHK
Israel	SI-32 Plug	CPK-9000-IL
Italy	CEI 23-16/VII Plug	CPK-9000-IT
Japan	JIS 8303 PSE Plug	CPK-9000-JP
Malaysia	BS1363/A Plug	CPK-9000-UKHK
Middle East	CEE 7/7 Plug	CPK-9000-CEE
New Zealand	AS/NZS 3112 Plug	CPK-9000-AUNZ
Norway	CEE 7/7 Plug	CPK-9000-CEE
Russia	CEE 7/7 Plug	CPK-9000-CEE
Singapore/Brunei	BS1363/A Plug	CPK-9000-UKHK
South Africa	BS 546 Plug	CPK-9000-ZAIN
Sweden	CEE 7/7 Plug	CPK-9000-CEE
Switzerland	SEV 1011 Plug	CPK-9000-CH
Tasmania	AS/NZS 3112 Plug	CPK-9000-AUNZ
United Kingdom	BS1363/A Plug	CPK-9000-UKHK

Environmental

Table A-7. Environmental Specifications

Temperature	
■ Operating	5 to 40°C (41 to 104°F)
■ Non-operating	-20 to 70°C (-4 to 158°F)
Humidity	
■ Operating	10% to 90%, non-condensing
■ Non-operating	10% to 95%, non-condensing
Altitude	
■ Operating	0 to 3048 m (0 to 10,000 feet)
■ Non-operating	0 to 15,240 m (0 to 50,000 feet)
Vibration	IEC 68-2-6,5
■ Operating	5 - 500 Hz, 0.2 g, 3 axis, dwell
■ Non-operating	2 - 200 Hz, 0.6 g, 3 axis, dwell
Shock	IEC 68-2
■ Operating	4 g, 11 ms, half sine, 20 repetitions/axis
■ Non-operating	30 g, 13 msec., 3 axis
Air flow	Front-to-back or back-to-front

Regulatory Certifications

Table A-8. Regulatory Certifications

Safety Standards	UL 60950-1 (USA) cUL 60950-1 (Canada) DEMKO and GS EN60950-1:2001, CE (Europe) CB Scheme: IEC 60950-1 (2001) GOST-R (Russia)
Emissions Standards	FCC Part 15 Class A ICES-003 Issue 4 VCCI Class A ITE CISPR 22, Class A EN 55022, Class A AS/NZS CISPR 22
Voltage Fluctuations	EN 61000-3-3
Harmonics	EN 61000-3-2
Immunity	EN 55024
Marking	UL_{US} (United States) cUL (Canada) CE (Europe) UL/GS (Europe) DEMKO (Europe)

Glossary

Active Zone Set

The zone set that defines the current zoning for the fabric.

Active Firmware

The firmware image on the switch that is in use.

Activity LED

A port LED that indicates when frames are entering or leaving the port.

Administrative State

State that determines the operating state of the port, I/O blade, or switch. The configured administrative state is stored in the switch configuration. The configured administrative state can be temporarily overridden using the command line interface.

Alarm

A message generated by the switch that specifically requests attention. Alarms are generated by several switch processes. Some alarms can be configured.

Alias

A named set of ports or devices used to make defining zone set membership easier. An alias is not a zone, and can not have a zone or another alias as a member.

AL_PA

Arbitrated Loop Physical Address

Arbitrated Loop

A Fibre Channel topology where ports use arbitration to establish a point-to-point circuit.

Arbitrated Loop Physical Address (AL_PA)

A unique one-byte value assigned during loop initialization to each NL_Port on a loop.

ASIC

Application Specific Integrated Circuit. A chip designed for a specific applications, such as a transmission protocol or a computer.

BootP

Boot Strap Protocol. A type of network server.

Buffer Credit

A measure of port buffer capacity equal to one frame.

Cascade Topology

A fabric in which the switches are connected in series. If you connect the last switch back to the first switch, you create a cascade-with-a-loop topology.

Challenge-Handshake Authentication Protocol

An authentication protocol by which a device is challenged to verify its identity before being allowed to log in to a switch.

Chassis Hop

A measure of fabric latency represented by the ISL that any frame crosses when travelling from one switch to another. A frame that travels from one switch to another over an ISL experiences one chassis hop.

Class 2 Service

A service which multiplexes frames at frame boundaries to or from one or more N_Ports wit h acknowledgment provided.

Class 3 Service

A service which multiplexes frames at frame boundaries to or from one or more N_Ports without acknowledgment.

Common Information Model

Switch service that provides for switch management through third-party applications that comply with SMI-S.

Configuration Wizard

An Enterprise Fabric Suite 2007 or QuickTools wizard that automates the switch configuration process.

Configured Zone Sets

The zone sets stored on a switch excluding the active zone set.

Domain ID

User defined number that identifies the switch in the fabric.

Enterprise Fabric Suite 2007

A separately licensed workstation-based switch management application.

Event Log

Log of messages describing events that occur in the fabric.

Expansion Port

E_Port that connects to another FC-SW-2 compliant switch.

Extended Credits

A feature of Enterprise Fabric Suite 2007 that enables you to reallocate port buffer credits to extend transmission distances.

Fabric Database

The set of fabrics that have been opened during a management session.

Fabric Management Switch

The switch through which the fabric is managed.

Fabric Name

User defined name in QuickTools and Enterprise Fabric Suite 2007 associated with the file that contains user list data for the fabric.

Fabric Port

An F_Port or FL_Port.

Fabric Security

A licensed feature that provides security for fabric users and devices including user account security and fabric services.

Fabric Services

A component of fabric security that provides for the control of inband management and SNMP on a switch.

Fabric View File

A file containing a set of fabrics that were opened and saved during a previous QuickTools or Enterprise Fabric Suite 2007 session.

Flash Memory

Memory on the switch that contains the chassis control firmware.

Frame

Data unit consisting of a start-of-frame (SOF) delimiter, header, data payload, CRC, and an end-of-frame (EOF) delimiter.

FRU

Field Replaceable Unit

Heartbeat LED

A chassis LED that indicates the status of the internal switch processor and the results of the Power-On Self-Test.

Inband Management

The ability to manage a switch through another switch over an inter-switch link.

Initiator

The device that initiates a data exchange with a target device.

In-Order-Delivery

A feature that requires that frames be received in the same order in which they were sent.

Input Power LED

A chassis LED that indicates that the switch logic circuitry is receiving proper DC voltages.

Inter-Switch Link

The connection between two switches using E_Ports.

IP

Internet Protocol

License Key

A code associated with a separately-purchased feature that activates that feature on the switch.

LIP

Loop Initialization Primitive sequence

Maintenance Button

Momentary button on the switch used to reset the switch or place the switch in maintenance mode.

Maintenance Mode

Maintenance mode sets the IP address to 10.0.0.1 and provides access to the switch for maintenance purposes.

Management Information Base

A set of guidelines and definitions for SNMP functions.

Management Workstation

PC workstation that manages the fabric through the fabric management switch.

Mesh Topology

A fabric in which each chassis has at least one port directly connected to each other chassis in the fabric.

MIB

Management Information Base

mPort Technology

Licensed feature that enables you to choose which Fibre Channel ports are active on a switch that is licensed for fewer than twenty ports.

Multistage Topology

A fabric in which two or more edge switches connect to one or more core switches.

Network Time Protocol

A network protocol that enables a client to synchronize its time with a server.

NL_Port

Node Loop Port. A Fibre Channel device port that supports arbitrated loop protocol.

N_Port

Node Port. A Fibre Channel device port in a point-to-point or fabric connection.

NTP

Network Time Protocol

Pending Firmware

The firmware image that will be activated upon the next switch reset.

Port Activation

A licensed feature that enables you to activate additional FC ports.

Port Binding

An authorization method that defines a list of device WWNs that can login to a switch port.

POST

Power-On Self Test

Power-On Self Test

Diagnostics that the switch chassis performs at start up.

Principal Switch

The switch in the fabric that manages domain ID assignments.

QuickTools

Browser-based switch management application that resides in the switch firmware.

Remote Authentication Dial-in Server

A server that supports the remote authentication of user and device logins to a switch.

SANdoctor

A licensed feature that provides for media diagnostics, Fibre Channel trace, and Fibre Channel ping functions.

Secure Shell

Protocol that secures connections to the switch for the command line interface.

Secure Socket Layer

Protocol that secures connections to the switch for Enterprise Fabric Suite 2007, QuickTools, the API, and SMI-S.

Security Set

A set of up to three groups that define device security for the switch.

Simple Network Management Protocol

An application protocol that manages and monitors network communications and functions. It also controls the Management Information Base (MIB).

SFP

Small Form-Factor Pluggable.

Small Form-Factor Pluggable

A transceiver device, smaller than a GigaBit Interface Converter, that plugs into the Fibre Channel port.

SMI-S

Storage Management Initiative–Specification.

SNMP

Simple Network Management Protocol

Stacking Cable

An XPAK cable that you use to connect two or more switches through the 10-Gbps ports.

Storage Management Initiative–Specification

A standard that provides for the management of the switch through third-party management applications.

Target

A storage device that responds to an initiator device.

User Account

An object stored on a switch that consists of an account name, password, authority level, and expiration date.

User Account Security

A component of fabric security that provides for the administration and authentication of account names, passwords, expiration dates, and authority level.

VCCI

Voluntary Control Council for Interference

Voluntary Control Council for Interference

A consortium of Japanese electronics industry associations that have established voluntary standards for controlling electromagnetic interference (EMI).

Worldwide Name (WWN)

A unique 64-bit address assigned to a device by the device manufacturer.

WWN

Worldwide Name

Zone

A set of ports or devices grouped together to control the exchange of information.

Zone Set

A set of zones grouped together. The active zone set defines the zoning for a fabric.

Zoning Database

The set of zone sets, zones, and aliases stored on a switch.

Notes

Index

Numerics

10/100 Base-T straight cable 4-12

A

account name
  default 4-13
  FTP 4-18
  maintenance mode 5-13
active zone set 3-2
Activity LED 2-5, 2-7
air flow A-7
alias 3-2
altitude A-7
Application Programming Interface 2-11
authorization 3-18

B

bandwidth 3-3, A-3
boot loader 5-16
browser 4-2
buffer credit 3-3, A-3

C

cable
  10/100 Base-T 4-12
  10/100 Base-T crossover 4-12
  fibre optic 3-1
  null modem F/F DB9 4-12
  XPAK switch stacking 4-6
Call Home service 3-15
cascade topology 3-11
certificate 3-16
chassis
  air flow A-7
  diagnostics 5-1
  marking A-8
  shock A-7
  vibration A-7
classes of service A-2
command line interface 2-10
Common Information Model 3-15
configuration
  file system error 2-3, 5-5, 5-6
  remove 5-15
  restore default 5-15
controls 2-2
credits 3-3, A-3
critical error 5-3

D

device
  access 3-2
  authentication 3-18
  authorization 3-18
  cabling 4-14
  description 3-1
  performance 3-6
  security 3-18
  security example 3-19
diagnostics 5-1, 5-3, A-4
dimensions A-5
distance 3-3

domain ID
  conflict 5-8
  description 3-7
  lock 3-7

E

E_Port 2-6, 5-8
e-mail notification 3-15
emissions standards A-8
environmental
  conditions 4-2
  specifications A-7
error
  critical 5-3
  fatal POST 5-4
  port 5-9
Ethernet
  direct connection 4-12
  indirect connection 4-12
  port 2-7

F

F_Port 2-6
fabric
  management A-4
  management workstation 4-2
  point-to-point bandwidth A-3
  port 2-6
  security 3-15
factory defaults 5-15
fiber optic cable 3-1
Fibre Channel
  ports 2-4
  protocols A-2
Field Replaceable Unit 6-1, A-4
File Transfer Protocol
  account name 4-18
  description 2-11
  service 3-15
firmware
  description 4-15
  failure 5-4
  install with CLI 4-16
  install with QuickTools 4-16
  non-disruptive activation 4-15
  unpack image 5-14
five-switch stacking 3-9
FL_Port 2-6
flash memory 2-3
four-switch stacking 3-9
frame size A-3
FRU - See Field Replaceable Unit
FTP - See File Transfer Protocol

G

G_Port 2-6
generic ports 2-6
GL_Port 2-6

H

harmonics A-8
HBA - See Host Bus Adapter
Heartbeat LED 2-2, 5-3
heat output A-5
host authentication example 3-26
host bus adapter 3-1
humidity 4-2, A-7
HyperTerminal application 4-8

I

immunity A-8
inband management 3-14
Input Power LED 5-2
installation 4-3
internal firmware failure 5-4
internet browser 4-2

L

latency 3-4, A-3
LED
  Activity 2-5, 2-7
  Heartbeat 2-2, 5-3
  Input Power 2-2, 5-2
  Link Status 2-7
  Logged-In 2-5, 5-7
  power supply 2-9
  System Fault 2-2, 5-2
license key 4-19
Link Status LED 2-7
log file 5-15
Logged-In LED 2-5, 5-7
login limit 3-28

M

maintainability A-4
maintenance
  interface A-4
  menu 5-14
  mode 2-3, 5-3, 5-13
Maintenance button 2-2, 2-3, 5-13
Management Server 3-15
management workstation 2-7, 4-12
marking A-8
media type A-3
memory
  flash 2-3
  workstation 4-2
mesh topology 3-12
minicom 4-8
multiple chassis fabrics 3-6
Multistage topology 3-13

N

new features 1-2
non-critical error 5-3
non-disruptive activation 4-15
NTP - See Network Time Protocol
null modem F/F DB9 cable 4-12

O

operating systems 4-2
over temperature 5-6

P

password
  file reset 5-15
  maintenance mode 5-13
  restore default 5-15
performance
  device 3-6
  switch 3-3
planning 3-1
port
  binding 3-17
  buffer credits 3-3
  characteristics A-2
  diagnostics 5-7
  Ethernet 2-7
  fabric 2-6
  Fibre Channel 2-4
  generic 2-6
  LEDs 2-5
  maximum number of ports/users A-3
  number of A-2
  security 3-17
  serial 2-8
  SFP 2-4
  speed A-3
  types 2-6, A-2
  XPAK 2-4
POST - See Power-on Self Test

power
  consumption A-5
  cord 4-10, A-5
  requirements 4-2
  source loading A-5
  supply 6-2
  supply diagnostics 5-12
Power Supply Fault LED 2-9, 5-12
Power Supply Status LED 2-9, 5-12
Power-on Self Test
  description 5-3
  fatal error 5-4
principal
  priority 3-7
  switch 3-7
processor 4-2, A-3

Q

QuickTools
  service 3-14
  web applet 2-10

R

rack mount 4-4
RADIUS - See Remote Dial-In User Service.
recovering a switch 5-13
regulatory certifications A-8
remake filesystem 5-16
Remote Dial-In User Service
  server authentication 3-17, 3-18
  server example 3-22
removal/replacement 6-1
RS-232 port 2-8
rubber feet 4-3

S

safety standards A-8
scalability A-3
Secure Shell
  description 3-16
  service 3-14
Secure Socket Layer service 3-14
security
  certificate 3-16
  connection 3-16
  database limits 3-18
  device 3-18
  fabric 3-15
  user account 3-17
serial port 2-8, 4-8, 4-12
SFP - See Small Form-Factor Pluggable
shock A-7
Simple Mail Transfer Protocol 3-15
Simple Network Management Protocol
  description 2-11
  service 3-14
site requirements 4-1
six-switch stacking 3-10
small form-factor pluggable
  port 2-4
  transceiver 2-6, 4-5, 6-2
SMI-S - See Storage Management Initiative-Specification
SMTP - See Simple Mail Transfer Protocol
SNMP - See Simple Network Management Protocol
soft zone 3-2
SSH - See Secure Shell
SSL - See Secure Socket Layer
stacking 3-6, 3-8
Storage Management Initiative-Specification 2-11
switch
  add to fabric 4-19
  configuration 4-13
  management 2-10
  management service 3-14
  power up 4-11
  recovery 5-13
  reset 2-3, 5-16
  services 3-14
  specifications A-2

System Fault LED 2-2, 5-2
system processor A-3

T

table mount 4-4
Telnet service 3-14
temperature
  error 5-6
  operating range 4-2, A-7
three-switch-stacking 3-8
timeout values 5-8
topology
  cascade 3-11
  mesh 3-12
  Multistage 3-13
transceiver 2-6, 4-5, 6-2
transmission rate 3-3
two-switch stacking 3-8

U

user account security 3-17
user interface A-4

V

vibration A-7
voltage
  fluctuations A-8
  operating A-5

W

web applet
  description 2-10
  service 3-14
workstation
  configuration 4-7
  connect 4-12
  IP address 4-7
  requirements 4-2

X

XPAK port 2-4

Z

zone
  conflict 5-9
  definition 3-2
zone set
  active 3-2
  definition 3-2
zoning
  database 3-2
  hardware enforced 3-2
  limits 3-2

Notes